ŁĄCZNOŚĆ BEZOSOBOWA I SIATKI PROXY

Rosyjska agentura w Europie od Kominternu do roku 2026

Opracowanie analityczno-szkoleniowe

dla kontrwywiadu, bezpieczeństwa organizacji
i ochrony infrastruktury krytycznej

Matthew Halaba

halaba.online

Materiał defensywny (white-hat)

Wydanie pierwsze, stan na wrzesień 2026

Publikacja bezpłatna

Tę książkę można pobierać, czytać i przekazywać dalej za darmo. Wiedza, która pomaga się bronić, ma krążyć bez opłaty.

Jeśli uznasz, że była coś warta, możesz postawić mi kawę:

buycoffee.to/maha

Autor: Matthew Halaba • halaba.online

Materiał defensywny (white-hat). Nie stanowi porady prawnej.

Spis treści

Od autora **1**

NOTA REDAKCYJNA I ZASTRZEŻENIE **2**

JAK KORZYSTAĆ Z TEGO OPRACOWANIA **3**

SŁOWNIK POJĘĆ I SKRÓTÓW **4**
Skróty służb i instytucji 5

CZĘŚĆ I. TŁO HISTORYCZNE, ŁĄCZNOŚĆ BEZOSOBOWA W PROGRAMIE NIELEGAŁÓW **6**

Rozdział 1. Czym jest łączność bezosobowa i dlaczego powstała **7**
Problem, który łączność bezosobowa miała rozwiązać 7
Trzy funkcje, które musiała spełniać 7
Dlaczego to działało przez dekady 8
Wniosek dla czytelnika defensywnego 8

Rozdział 2. Od bolszewickiego podziemia do Zarządu S **9**
Konspiracja jako gen założycielski 9
Wydział, który prowadził nielegałów 9
Cena, jaką płacili ludzie 10
Wniosek 10

Rozdział 2a. Motywacje: dlaczego ludzie podejmują współpracę **11**
Model MICE 11
Dlaczego to ma znaczenie dla obrony 11
Nowa motywacja: nieświadomość 12

Rozdział 3. Anatomia klasycznej martwej skrzynki, spojrzenie z perspektywy śledczego **13**
Co śledczy w ogóle szuka 13
Trzy elementy, które musi powiązać śledczy 13
Dlaczego akurat ta perspektywa jest przydatna w 2026 roku 14

Rozdział 4. Cztery klasyczne sprawy **15**
Rudolf Abel (Wiliam Fisher), nielegał wzorcowy i jego upadek 15
Siatka z Portland, codzienność jako kamuflaż 15
Robert Hanssen, kret i łączność bezosobowa doprowadzona do perfekcji 15

Ghost Stories, dekada obserwacji i zdrada od wewnątrz 16
Wspólny mianownik czterech spraw 16

Rozdział 4a. Więcej z historii łączności bezosobowej 17
Archiwum Mitrochina, wartość jednego człowieka wewnątrz 17
Kult nielegała i jego cena 17
Ciągłość między epokami 17

Rozdział 5. Dlaczego systemy łączności się sypały 18
Podsumowanie Części I 18

CZĘŚĆ II. AKTUALIZACJA PO 2022, OD NIELEGAŁA DO AGENTA JEDNORAZOWEGO 20

Rozdział 6. Cezura lutego 2022 i załamanie rezydentur legalnych 21
Dzień, który przemeblował rosyjski wywiad w Europie 21
Dlaczego to wywołało falę sabotażu 21
Nowa geografia zagrożenia 22

Rozdział 6a. Szersze tło: środowisko bezpieczeństwa po 2022 roku 23
Wojna, która nie mieści się w dawnych kategoriach 23
Nowe fronty, ta sama logika 23
Zbieżność rozpoznania i ataku 24
Dlaczego akurat teraz warto szkolić 24

Rozdział 6b. Synergia, o której wszyscy zapomnieli 25
Jak wygląda pojedyncza operacja, gdy się jej przyjrzeć w całości 25
Dlaczego akurat teraz to boli 25
Co to znaczy dla obrony, konkretnie 26
Gdzie jest pułapka 26
Czego nie wiem 26

Rozdział 7. Powrót klasycznych nielegałów: Czerkasow, Dulcewowie, Kołobowa 27
Siergiej Czerkasow, nielegał zdemaskowany u progu celu 27
Dulcewowie, nielegałowie „z podręcznika” i ich koniec 27
Olga Kołobowa, „Maria Adela” z Neapolu 28
Wspólny wniosek trzech spraw 28

Rozdział 8. GRU, jednostka 29155 i przemysł sabotażu 29
Od pojedynczych operacji do systemu 29
Przemysł, nie pojedyncze akcje 29
Cele: logistyka wsparcia dla Ukrainy 30

Rozdział 9. Werbunek przez Telegram, anatomia maszyny 31
Ogłoszenie, od którego się zaczyna 31
Sześć faz, model SUPO 31
Dlaczego ten model jest dla Moskwy tak wygodny 32
Gdzie ten model jest słaby i to jest wiadomość dla obrońcy 32

Rozdział 10. Nośniki i płatności ery cyfrowej 33

Instrukcja: komunikator zamiast sygnału . . . 33
Pieniądze: kryptowaluta zamiast gotówki w skrzynce . . . 33
Przedmiot: łańcuch kurierski jako nośnik . . . 33
Rozpoznanie: dron i telefon zamiast fotografa . . . 34
Wniosek: nośniki nowe, logika stara . . . 34

Rozdział 11. Mapa kampanii 2022–2026 kraj po kraju 35
Polska, kraj frontowy hybrydowo . . . 35
Litwa, węzeł paczek zapalających i celownik na dysydentów . . . 35
Niemcy, od podpaleń po drony nad cargo . . . 36
Wielka Brytania, pierwsze wyroki z nowej ustawy . . . 36
Czechy, rozpoznanie werbunku migrantów . . . 36
Estonia, Łotwa, Norwegia, Włochy i inni . . . 36
Odczyt mapy dla polskiej firmy . . . 36

Rozdział 11a. Profile krajowe, rozszerzenie 37
Polska, laboratorium zagrożenia i odpowiedzi . . . 37
Niemcy, połączenie ścigania i uświadamiania . . . 37
Wielka Brytania, nowe prawo w działaniu . . . 37
Kraje bałtyckie, pierwsza linia i pełne spektrum . . . 38
Kierunek morski, Bałtyk i infrastruktura podmorska . . . 38
Wniosek z profili . . . 38

Rozdział 12. Sześć spraw z bliska 39
12.1. Leyton, Londyn, podpalenie zlecone przez Wagnera (marzec 2024) . . . 39
12.2. Paczki zapalające DHL/DPD (lipiec 2024) . . . 39
12.3. Sabotaż kolejowy pod Mika i Puławami (listopad 2025) . . . 39
12.4. Siatka zabójstw i sabotażu rozbita z udziałem Ukrainy (2025–2026) . . . 40
12.5. Paczki z GPS śledzące logistykę (wyrok 2026) . . . 40
12.6. Dulcewowie, koniec klasycznego nielegała (2022–2024) . . . 40

Rozdział 13. Dlaczego siatki proxy wpadają 41
Podsumowanie Części II . . . 41

CZĘŚĆ III. MODUŁ SZKOLENIOWY (DEFENSYWNY) 43

Rozdział 14. Cele, odbiorcy i zasady modułu 44
Po co ten moduł istnieje . . . 44
Kto jest odbiorcą . . . 44
Cztery zasady, które obowiązują przez cały moduł . . . 44
Format prowadzenia szkolenia . . . 45

Rozdział 15. Cykl werbunkowy w sześciu fazach 46
Faza 1, kontakt . . . 46
Faza 2, test . . . 46
Faza 3, eskalacja . . . 47
Faza 4, dowód wykonania . . . 47
Faza 5, zatrzymanie . . . 47
Faza 6, konsekwencje . . . 47

Diagram cyklu (do slajdu) . . . 47

Rozdział 16. Katalog sygnałów ostrzegawczych 48
Grupa A, sygnały werbunku (personel i osoby z zewnątrz) . . . 48
Grupa B, sygnały rozpoznania obiektu (hostile reconnaissance) . . . 48
Grupa C, sygnały łączności bezosobowej i podłożenia . . . 48
Grupa D, sygnały głębokiego przykrycia (nielegał) . . . 49

Rozdział 17. Karty pracy i listy kontrolne 50
Karta 1, Obserwacja podejrzanego zachowania (dla ochrony) . . . 50
Karta 2, Podejrzany przedmiot / przesyłka (dla ochrony i personelu) . . . 50
Karta 3, Zgłoszenie próby werbunku (dla personelu) . . . 51
Lista kontrolna A, Przyjmowanie przesyłek w obiekcie chronionym . . . 51
Lista kontrolna B, Higiena dostępu i informacji o obiekcie . . . 51
Lista kontrolna C, Insider risk (model NPSA, w skrócie) . . . 51

Rozdział 18. Ćwiczenia sztabowe (tabletop) na realnych sprawach 52
Ćwiczenie 1, Magazyn (na kanwie Leyton 2024) . . . 52
Ćwiczenie 2, Przesyłka (na kanwie paczek DHL 2024) . . . 52
Ćwiczenie 3, Kolej / infrastruktura liniowa (na kanwie Mika/Puławy 2025) . . . 53
Ćwiczenie 4, „Szara myszka” (na kanwie Dulcewów) . . . 53
Jak prowadzić i podsumować . . . 53

Rozdział 19. Postępowanie po wykryciu, eskalacja i zgłoszenie 54
Łańcuch reakcji w pięciu krokach . . . 54
Czego nie robić, katalog błędów . . . 54
Rola organizacji między incydentami . . . 55

Moduł dodatkowy A. Wykrywanie wrogiego rozpoznania wokół placówki (Surveillance Detection, od strony obrońcy) 56
Dlaczego rozpoznanie poprzedza atak . . . 56
Cykl wrogiego rozpoznania (do rozpoznania, nie do naśladowania) . . . 56
Wskaźniki wrogiego rozpoznania . . . 56
Metoda obrońcy: znać normę, budować pamięć, korelować . . . 57

Moduł dodatkowy B. Ochrona placówki i reagowanie na podejrzany przedmiot 58
Warstwy ochrony obiektu . . . 58
Kontrola dostępu, zasady . . . 58
Przyjmowanie przesyłek, po kampanii paczek 2024 . . . 58
Reagowanie na podejrzany przedmiot, protokół 4×NIE + 3×TAK . . . 58
Współpraca ze służbami . . . 59

Rozdział 20. Test wiedzy i klucz odpowiedzi 60
Pytania . . . 60
Klucz odpowiedzi (z komentarzem) . . . 60
Podsumowanie Części III . . . 61

CZĘŚĆ IV. STRONA KONTRWYWIADOWCZA I SYSTEMOWA 62

Rozdział 21. Jak służby rozbijały siatki 63

Sześć dźwigni wykrywania . . . 63
Kolejność, która się powtarza . . . 63

Rozdział 21b. Anatomia śledztwa: jak rozplata się sprawę synergiczną 64

Rozdział 21c. Cyber jako jedna z warstw, nie cała wojna 66

Rozdział 22. Ramy prawne po 2022 roku 67
Wielka Brytania, National Security Act 2023 . . . 67
Niemcy, ściganie i ostrzeganie . . . 67
Polska, sabotaż, dywersja, szpiegostwo . . . 67
Poziom Unii Europejskiej, sankcje za zagrożenia hybrydowe . . . 67
Wniosek dla obrońcy . . . 68

Rozdział 23. Kampanie uświadamiające jako narzędzie kontrwywiadu 69
Nowa broń: milion czujników . . . 69
Przegląd kampanii . . . 69
Dlaczego to działa . . . 69

Rozdział 24. Odporność organizacji i infrastruktury krytycznej 70
Od reagowania do odporności . . . 70
Sześć filarów odporności organizacyjnej . . . 70
Specyfika infrastruktury rozproszonej . . . 70
Miara dojrzałości . . . 71

Rozdział 24a. Odporność jako synergia, nie jako suma zabezpieczeń 72

Rozdział 24b. Personel miejscowy i ryzyko wewnętrzne na placówce podwyższonego ryzyka 73

Rozdział 24c. Dron nad obiektem: rozpoznanie i reakcja 75

Rozdział 25. Prognoza i wnioski 76
Dokąd to zmierza . . . 76
Trzy wnioski końcowe . . . 76
Podsumowanie Części IV . . . 77

CZĘŚĆ V. PRZEWODNIK METODYCZNY DLA PROWADZĄCEGO SZKOLENIE 78

Rozdział 26. Jak przygotować i poprowadzić szkolenie 79
Zasada nadrzędna: uczymy nawyku, nie wiedzy . . . 79
Zasada realizmu: pracujemy na prawdziwych sprawach . . . 79
Zasada bezpieczeństwa przekazu: linia obronna, nie ofensywna . . . 79
Cztery komunikaty, które muszą zostać w głowie . . . 79

Rozdział 27. Plany sesji dla trzech poziomów odbiorców 81
Sesja dla poziomu 1, cały personel (90 minut) . . . 81
Sesja dla poziomu 2, ochrona i oficerowie bezpieczeństwa (1 dzień) . . . 81
Sesja dla poziomu 3, kadra kierownicza i analitycy (pół dnia) . . . 81
Wskazówki logistyczne . . . 82

Rozdział 28. Dodatkowe ćwiczenia i materiały warsztatowe **83**
Ćwiczenie „niewinne czy podejrzane?” (rozgrzewka, 15 min) . . . 83
Ćwiczenie tabletop 5, Placówka dyplomatyczna (dla poziomu 2/3) . . . 83
Ćwiczenie tabletop 6, Węzeł logistyczny wsparcia (dla poziomu 2) . . . 84
Karta uczestnika, „Moje trzy zobowiązania” . . . 84

Rozdział 29. Mity i fakty oraz najczęstsze pytania uczestników **85**
Mity i fakty . . . 85
Najczęstsze pytania . . . 85

Rozdział 30. OPSEC obrońcy: jak nie oddać przeciwnikowi tego, czego sam szuka **87**
Co przeciwnik zbiera, zanim w ogóle się pojawi . . . 87
Higiena informacji jawnej . . . 87
Ochrona ludzi . . . 88
Ochrona kanału zgłoszeń . . . 88
Higiena cyfrowa bez magii . . . 88
Czego nie wiem . . . 88

Rozdział 31. Sektor prywatny i infrastruktura krytyczna: dlaczego to już wasza sprawa **89**

Rozdział 32. Dziesięć rzeczy do zapamiętania **90**

DODATKI **91**

Dodatek A. Kalendarium incydentów 2022–2026 **92**

Dodatek B. Struktura rosyjskich służb specjalnych (w zakresie istotnym dla tematu) **94**

Dodatek C. Zbiorcza karta wskaźników rozpoznania (do wydruku) **95**

Dodatek D. Bibliografia i źródła **96**

Przypisy **98**

Od autora

Stan na wrzesień 2026.

Piszę to jako cywil i analityk z terenu, nie jako oficer i nie jako naukowiec. Zajmuję się OSINT-em, odpornością cywilną i technologiami podwójnego zastosowania, jeżdżę tam, gdzie widać wojnę z bliska i od kilku lat patrzę, jak rosyjski wywiad przestawia się z jednej metody na drugą. Ta książka wzięła się z lektury Shauna Walkera o nielegałach i z prostego pytania, które sam sobie zadałem: skoro klasyczna martwa skrzynka odchodzi do historii, to co weszło na jej miejsce i jak to rozpoznać.

Od razu mówię, czego tu nie ma, żeby nie było nieporozumień. Nie ma instrukcji zakładania i podejmowania skrzynek. Nie ma doboru miejsc pod monitoring, budowy pojemników, protokołów sygnałowych ani tras omijania obserwacji. To jest wiedza wykonawcza i nie służy obronie. Trzymam się zasady, której trzymam się we wszystkim, co publikuję: analiza nie jest instrukcją. Opisuję metodę przeciwnika po to, żeby ją wykryć, nie po to, żeby ją odtworzyć. Kto szuka poradnika dla siatki, trafił źle.

Pierwszy wniosek stawiam na początku, bo tak wolę pisać. Po 24 lutego 2022 roku przewaga wróciła do obrońcy, tylko trzeba ją wziąć. Przez dekady klasyczna łączność bezosobowa dawała przewagę atakującemu, bo była prawie nie do złamania od zewnątrz. Era danych to odwróciła. Przeciwnik zszedł na masowy, cyfrowy model pośredników i agentów jednorazowych, zyskał skalę i zaprzeczalność, ale stracił niewidzialność. Każdy nowy nośnik zostawia ślad, którego cegła w murze nie zostawiała. To realna przewaga, pod jednym warunkiem: że po stronie obrony jest przeszkolony człowiek, który wychwyci pierwszy sygnał i zgłosi go tak, jak trzeba.

Piszę fakt jako fakt, ocenę jako ocenę, a spekulację nazywam po imieniu albo ją wycinam. Fakty mają źródło i datę, wypisałem je w przypisach i bibliografii. Tam, gdzie mówię „oceniam”, to jest moja ocena z terenu i z lektury akt, nie prawda objawiona. Sprawy będące w toku opisuję z domniemaniem niewinności, a stan wiedzy podaję na wrzesień 2026 i wiem, że się zestarzeje.

Konflikt interesów wykładam od razu, bo czytelnik ma prawo wiedzieć, skąd patrzę: pracuję w bezpieczeństwie, robię w OSINT i w odporności i część tego, co opisuję, dotyka obszarów, w których mam projekty. Nie zmienia to faktów, ale zmienia to, na co zwracam uwagę.

Czego nie wiem, piszę wprost w środku, przy każdej sprawie, a zbiorczo w rozdziale prognostycznym. Nie wiem, ilu nielegałów wciąż siedzi cicho w Europie. Nie wiem, ile siatek proxy działa poza zasięgiem służb. Nie wiem, jak szybko przeciwnik zredukuje ślady, które dziś go zdradzają. Analiza bez luk to marketing, więc luki zostawiam widoczne.

Książkę zrobiłem darmową, bo uważam, że wiedza, która pomaga się bronić, ma krążyć bez opłaty. Jeśli uznasz, że była coś warta, możesz postawić mi kawę: buycoffee.to/maha. Nic poza tym.

Matthew Halaba halaba.online

NOTA REDAKCYJNA I ZASTRZEŻENIE

Niniejsze opracowanie powstało jako rozwinięcie i aktualizacja wątku łączności bezosobowej opisanego w książce Shauna Walkera *Nielegałowie. Jak szpieguje nas Rosja*. Punktem wyjścia jest historia radzieckiego i rosyjskiego programu nielegałów, agentów działających bez przykrycia dyplomatycznego, pod obcą tożsamością, a w szczególności sposób, w jaki tacy agenci utrzymywali kontakt z Centralą bez bezpośredniego spotkania: przez łączność bezosobową, w tym tak zwane martwe skrzynki kontaktowe.

Czym to opracowanie jest. Jest to analiza zjawiska i podręcznik jego rozpoznawania. Opisuje, jak historycznie działała łączność bezosobowa, dlaczego rosyjskie służby po niej sięgały, jak kolejne systemy były wykrywane i rozbijane, oraz, co najważniejsze dla czytelnika w 2026 roku, jak ten model wyewoluował po pełnoskalowej inwazji Rosji na Ukrainę w lutym 2022 roku w kierunku siatek jednorazowych wykonawców werbowanych przez komunikatory. Część szkoleniowa uczy rozpoznawać wzorce werbunku i przekazu, czytać sygnały ostrzegawcze w organizacji i reagować na nie zgodnie z prawem.

Czym to opracowanie nie jest. Nie jest instrukcją operacyjną dla osoby, która miałaby zakładać lub podejmować martwą skrzynkę. Świadomie i konsekwentnie nie zawiera treści wykonawczych, które służyłyby ukryciu takiej działalności przed wykryciem: doboru konkretnych miejsc pod kątem omijania monitoringu, konstrukcji pojemników maskujących, protokołów sygnalizacji „załadowano / podjęto", tras i technik wykrywania obserwacji, harmonogramów pod unikanie namierzenia telekomunikacyjnego. Tego rodzaju wiedza, niezależnie od intencji zamawiającego, jest w praktyce instrukcją dla siatki agenturalnej albo dla przestępczości zorganizowanej i w tym opracowaniu jej nie ma. Perspektywa jest tu odwrócona: wszędzie tam, gdzie opisujemy metodę przeciwnika, robimy to po to, żeby ją rozpoznać i udaremnić, a nie odtworzyć.

Źródła. Opracowanie opiera się wyłącznie na materiałach jawnych: książce Walkera, odtajnionych aktach służb, publicznych aktach oskarżenia i komunikatach prokuratur, raportach agencji bezpieczeństwa (m.in. ABW, niemieckich BKA/BfV/BND, fińskiej SUPO, czeskiej BIS), publikacjach ośrodków analitycznych oraz dziennikarstwie śledczym opartym na otwartych źródłach (OSINT), w tym pracach grupy Bellingcat. Pełny wykaz znajduje się w bibliografii i przypisach. Tam, gdzie źródła są niepewne lub sprzeczne, jest to zaznaczone.

Odbiorca i sposób wykorzystania. Materiał jest przeznaczony do legalnego użytku obronnego: szkolenia personelu, budowania odporności organizacji, wspierania pracy analityków i śledczych. Nie stanowi porady prawnej. Procedury zgłaszania i eskalacji należy każdorazowo dostosować do obowiązującego prawa krajowego i wewnętrznych regulacji organizacji.

JAK KORZYSTAĆ Z TEGO OPRACOWANIA

Opracowanie ma budowę modułową i można je czytać na kilka sposobów.

Czytelnik, który chce zrozumieć zjawisko całościowo, powinien czytać po kolei. Część I buduje słownik pojęć i pokazuje, skąd wzięła się łączność bezosobowa oraz dlaczego przez dekady była filarem programu nielegałów. Część II pokazuje, jak ten model załamał się i przekształcił po 2022 roku. Dopiero na tym tle części III i IV, szkoleniowa i kontrwywiadowcza, nabierają pełnego sensu.

Oficer bezpieczeństwa lub prowadzący szkolenie, który potrzebuje gotowego materiału warsztatowego, może przejść od razu do Części III. Znajdzie tam cykl werbunkowy rozpisany na fazy, katalog sygnałów ostrzegawczych, karty pracy, cztery scenariusze ćwiczeń sztabowych oparte na rzeczywistych sprawach oraz test wiedzy z kluczem. Do prowadzenia zajęć warto jednak wcześniej przeczytać Część II, bo scenariusze odwołują się do konkretnych spraw.

Analityk lub śledczy znajdzie najwięcej w częściach II i IV: w rekonstrukcji modelu werbunku i łączności oraz w opisie metod, którymi europejskie służby te siatki wykrywały i rozbijały.

Kadra zarządzająca i decydenci mogą ograniczyć się do rozdziałów 6, 11, 13, 24 i 25 oraz do kalendarium w Dodatku A, dają one obraz skali zagrożenia i kierunku jego ewolucji bez wchodzenia w szczegóły warsztatowe.

W tekście stosujemy trzy powtarzalne elementy graficzne:

> **RAMKA FAKTOGRAFICZNA.** Zwięzłe zestawienie ustalonych faktów w danej sprawie: kto, co, kiedy, z jakim skutkiem prawnym.

> **SYGNAŁ OSTRZEGAWCZY.** Wskaźnik, który w praktyce pozwalał rozpoznać werbunek, łączność bezosobową albo przygotowania do sabotażu, zanim doszło do szkody.

> **UWAGA OPSEC.** Przypomnienie o granicy tego opracowania: dlaczego w danym miejscu świadomie pomijamy szczegóły wykonawcze i co to oznacza dla czytelnika.

Każda część kończy się krótkim podsumowaniem najważniejszych wniosków.

SŁOWNIK POJĘĆ I SKRÓTÓW

Nielegał (ros. *nielegał*), oficer wywiadu lub agent działający za granicą bez przykrycia dyplomatycznego, pod fałszywą tożsamością (często obywatelstwa państwa trzeciego). W odróżnieniu od rezydenta „legalnego" nie ma immunitetu i w razie dekonspiracji odpowiada karnie jak zwykły przestępca. Budowa wiarygodnej „legendy" nielegała zajmowała historycznie wiele lat.

Rezydentura legalna, komórka wywiadu działająca pod przykryciem oficjalnej placówki (najczęściej ambasady lub konsulatu). Oficerowie mają status dyplomatyczny i immunitet; w razie dekonspiracji są zwykle wydalani jako *persona non grata*, a nie sądzeni.

Legenda, spójna fałszywa biografia i tożsamość, wraz z dokumentami i „historią życia", która ma wytrzymać weryfikację.

Łączność bezosobowa, sposób przekazywania informacji, pieniędzy lub przedmiotów między agentem a prowadzącym bez ich fizycznego spotkania. Historycznym narzędziem łączności bezosobowej była martwa skrzynka kontaktowa. Współcześnie funkcję tę w dużej mierze przejęły kanały cyfrowe i pośrednicy.

Martwa skrzynka kontaktowa (ang. *dead drop*), uzgodnione miejsce, w którym jedna osoba pozostawia przesyłkę, a druga podejmuje ją w innym czasie, dzięki czemu obie nigdy się nie spotykają. W tym opracowaniu opisujemy ją jako zjawisko i przedmiot rozpoznania, nie podajemy natomiast instrukcji jej zakładania.

Żywa skrzynka (ang. *live drop*), przekazanie „z ręki do ręki", zwykle zamaskowane jako przypadkowy lub codzienny kontakt.

Sygnał, umówiony, z pozoru niewinny znak informujący drugą stronę, że nastąpiło określone zdarzenie (np. że przesyłka jest gotowa do podjęcia). Opisujemy istnienie tego mechanizmu; nie podajemy gotowych protokołów.

Agent jednorazowy / „agent do wyrzucenia" (ang. *disposable agent*, niem. *Wegwerf-Agent*, *Low-Level-Agent*), osoba zwerbowana do pojedynczego zadania (obserwacji, podpalenia, podłożenia ładunku, nadania przesyłki), zwykle przez komunikator, często nieświadoma, dla kogo naprawdę pracuje i pozbawiona jakiegokolwiek wsparcia po zatrzymaniu. Termin ukuty przez niemieckie służby w kampanii z 2025 roku.

Proxy, pośrednik lub wykonawca działający w interesie państwa, ale formalnie z nim niepowiązany, co pozwala Moskwie zaprzeczać sprawstwu (ang. *plausible deniability*).

Zagrożenie hybrydowe, działania poniżej progu otwartego konfliktu zbrojnego: sabotaż, dywersja, cyberataki, dezinformacja, instrumentalne wykorzystanie migracji, presja energetyczna, naruszenia przestrzeni powietrznej.

OSINT (ang. *Open-Source Intelligence*), biały wywiad; ustalanie faktów na podstawie źródeł ogólnodostępnych (rejestrów, mediów społecznościowych, zdjęć satelitarnych, wycieków danych).

MICE, klasyczny akronim opisujący motywacje osób podejmujących współpracę z obcym wywiadem: *Money* (pieniądze), *Ideology* (ideologia), *Coercion/Compromise* (przymus/szantaż), *Ego*.

Skróty służb i instytucji

SWR (ros. СВР), Służba Wywiadu Zagranicznego Federacji Rosyjskiej, spadkobierczyni Pierwszego Zarządu Głównego KGB; odpowiada m.in. za program nielegałów (historycznie: Zarząd „S”).

GRU (obecnie formalnie GU), wywiad wojskowy Federacji Rosyjskiej. Z GRU powiązana jest jednostka 29155, kojarzona z operacjami sabotażu i zabójstw za granicą.

FSB (ros. ФСБ), Federalna Służba Bezpieczeństwa; głównie kontrwywiad i bezpieczeństwo wewnętrzne, po 2022 roku coraz aktywniejsza również w operacjach zagranicznych, zwłaszcza na kierunku ukraińskim.

KGB, Komitet Bezpieczeństwa Państwowego ZSRR (do 1991), poprzednik SWR i FSB.

ABW, Agencja Bezpieczeństwa Wewnętrznego (Polska).

BfV / BKA / BND / BAMAD, niemieckie: Federalny Urząd Ochrony Konstytucji / Federalny Urząd Kryminalny / Federalna Służba Wywiadu / Wojskowa Kontrwywiadowcza.

SUPO, Fińska Służba Bezpieczeństwa i Wywiadu.

BIS, Służba Informacji Bezpieczeństwa (czeski kontrwywiad).

MI5 / CPS, brytyjska Służba Bezpieczeństwa / Koronna Służba Prokuratorska.

NPSA, brytyjska National Protective Security Authority (doradztwo w zakresie ochrony fizycznej i personalnej).

Eurojust / Europol, agencje UE ds. współpracy sądowej i policyjnej.

CZĘŚĆ I. TŁO HISTORYCZNE, ŁĄCZNOŚĆ BEZOSOBOWA W PROGRAMIE NIELEGAŁÓW

Rozdział 1. Czym jest łączność bezosobowa i dlaczego powstała

Problem, który łączność bezosobowa miała rozwiązać

Każda tajna współpraca sprowadza się w pewnym momencie do jednej niebezpiecznej czynności: dwie strony muszą coś sobie przekazać. Informację, pieniądze, dokument, sprzęt, instrukcję. W wywiadzie ten moment przekazania jest najsłabszym ogniwem całego przedsięwzięcia. Agent może latami żyć pod nienaganną legendą, ale w chwili, gdy spotyka się ze swoim oficerem prowadzącym, obie osoby znajdują się jednocześnie w jednym miejscu, a to jest właśnie ten kadr, którego szuka kontrwywiad. Jedno zdjęcie takiego spotkania potrafi przewrócić operację, która budowana była dekadę.

Łączność bezosobowa jest odpowiedzią na ten problem. Jej istotą jest rozdzielenie w czasie i przestrzeni czynności „zostawiam" i czynności „podejmuję", tak aby dwie współpracujące osoby nigdy nie znalazły się razem w jednym miejscu i w jednym momencie. Klasycznym narzędziem była martwa skrzynka kontaktowa: jedna osoba pozostawiała przesyłkę w umówionym miejscu, druga podejmowała ją później. Do tego dochodził system sygnałów, z pozoru niewinnych znaków, które informowały drugą stronę, że przesyłka czeka albo że została odebrana.

Dla kontrwywiadu oznaczało to fundamentalną trudność. Nie wystarczyło już ustalić, że osoba A jest szpiegiem. Trzeba było jeszcze powiązać ją z osobą B, mimo że te dwie osoby nigdy się nie widziały, nie dzwoniły do siebie, nie pisały. Cała architektura łączności bezosobowej służyła temu, by nawet w razie wpadki jednego ogniwa reszta siatki pozostała nietknięta.

> **UWAGA OPSEC.** W całym tym rozdziale i w całym opracowaniu, opisujemy *logikę* łączności bezosobowej: po co powstała i jaki problem rozwiązywała. Celowo nie podajemy, jak dobrać miejsce, jak zbudować pojemnik ani jak zaprojektować system sygnałów. Ta wiedza jest wykonawcza i nie ma defensywnego zastosowania: ochroniarz, analityk czy oficer bezpieczeństwa nie musi umieć zakładać skrzynki, żeby ją rozpoznać. Musi wiedzieć, *że* takie zjawisko istnieje, *jak się przejawia* i *jak zareagować* i temu poświęcona jest część szkoleniowa.

Trzy funkcje, które musiała spełniać

Historyk wywiadu, analizując zachowane akta, dostrzega, że dobrze zaprojektowana łączność bezosobowa realizowała jednocześnie trzy funkcje.

Po pierwsze, **rozdzielenie tożsamości**. Nadający i podejmujący mieli pozostać dla siebie anonimowi, najlepiej, żeby jeden nie znał nawet twarzy drugiego. Dzięki temu zatrzymanie jednego z nich nie prowadziło automatycznie do drugiego. Zasada ta, znana jako kompartmentalizacja, jest tym samym mechanizmem, który dziś w siatkach proxy realizuje się przez łańcuch pośredników na Telegramie, o czym w Części II.

Po drugie, **zaprzeczalność**. Sama przesyłka miała wyglądać niewinnie, a czynność jej pozostawienia, jak zwykły element codziennego życia. Chodziło o to, by nawet przyłapany „na gorącym uczynku” agent mógł twierdzić, że nic się nie stało. Ta sama logika zaprzeczalności napędza dziś rosyjskie operacje hybrydowe: państwo chce móc powiedzieć „to nie my”, a wykonawca, „nie wiedziałem, dla kogo pracuję”.

Po trzecie, **odporność na obserwację**. System zakładał, że przeciwnik patrzy i był tak zaprojektowany, by nawet obserwowany moment nie zdradzał, co naprawdę się dzieje. To założenie, „przeciwnik zawsze patrzy”, jest jednocześnie najlepszą wskazówką dla strony defensywnej: skoro operacja jest budowana pod obserwację, to znaczy, że cierpliwa, systematyczna obserwacja jest tym, co ją demaskuje.

Dlaczego to działało przez dekady

Łączność bezosobowa była skuteczna, dopóki świat był „analogowy”. W epoce, w której nie było powszechnego monitoringu miejskiego, rejestrów przekroczeń granic w czasie rzeczywistym, danych lokalizacyjnych z telefonów, rozpoznawania twarzy i płatności zostawiających cyfrowy ślad, ustalenie związku między dwojgiem ludzi, którzy nigdy się nie spotkali, było zadaniem graniczącym z niemożliwością. Kontrwywiad mógł mieć przeczucie, mógł nawet obserwować podejrzanego, ale przekucie przeczucia w dowód sądowy wymagało złapania kogoś dokładnie w momencie czynności, a cały system był zbudowany po to, by taki moment uczynić jak najrzadszym i jak najbardziej niejednoznacznym.

Ta przewaga zaczęła się kruszyć wraz z cyfryzacją, a ostatecznie załamała się w drugiej dekadzie XXI wieku. Rozdział 5 pokazuje, jak kolejne systemy łączności, wydawałoby się dopracowane przez dziesięciolecia, sypały się jeden po drugim. Część II pokazuje zaś, że skoro klasyczna łączność bezosobowa stała się w erze danych biometrycznych i cyfrowych śladów tak ryzykowna, przeciwnik nie tyle ją udoskonalił, ile zastąpił czymś innym: siatkami jednorazowych ludzi, sterowanych zdalnie, których „przekaz” odbywa się dziś częściej przez skrzynkę pocztową firmy kurierskiej i portfel kryptowalutowy niż przez cegłę w murze.

Wniosek dla czytelnika defensywnego

Zapamiętajmy trzy rzeczy, bo wracać będą przez całe opracowanie. Łączność bezosobowa istnieje po to, żeby rozdzielić ludzi, zapewnić zaprzeczalność i przetrwać obserwację. Każdą z tych trzech funkcji da się zaatakować od strony defensywnej i to jest właśnie zadanie kontrwywiadu i ochrony. Rozdzielenie ludzi pokonuje się przez łączenie śladów (dziś: cyfrowych). Zaprzeczalność pokonuje się przez cierpliwe budowanie kontekstu, który odbiera „niewinnemu” zachowaniu jego niewinność. Odporność na obserwację pokonuje się przez… obserwację, systematyczną, wielopunktową, wspartą danymi.

Rozdział 2. Od bolszewickiego podziemia do Zarządu S

Konspiracja jako gen założycielski

Rosyjski program nielegałów nie zaczął się od państwa, zaczął się od podziemia. Zanim bolszewicy przejęli władzę, działali jako nielegalna partia rewolucyjna: fałszywe nazwiska, konspiracyjne mieszkania, przemyt literatury i pieniędzy, życie w ciągłym ukryciu przed carską Ochraną. Kiedy w 1917 roku doszli do władzy, wnieśli tę kulturę konspiracji do aparatu państwowego. Umiejętność życia pod fałszywą tożsamością i utrzymywania łączności bez zdradzania się nie była dla nich abstrakcyjną techniką wywiadowczą, była nawykiem z lat podziemia.

To pochodzenie tłumaczy, dlaczego program nielegałów zajął w radzieckim wywiadzie miejsce niemal mityczne. Dla bolszewika nielegał był ideałem: człowiekiem, który dla sprawy porzuca własne nazwisko i całą biografię, przenosi się do wrogiego kraju i latami żyje w przebraniu. Walker w swojej książce pokazuje, jak ten kult przetrwał wszystkie epoki, od pierwszego wydziału nielegałów utworzonego przez Michaiła Trilissera w latach dwudziestych, przez czystki stalinowskie, które zdziesiątkowały pierwsze pokolenie, aż po współczesną SWR, której szef Siergiej Naryszkin w 2017 roku, przemawiając w Jasieniewie, wprost odwoływał się do dziedzictwa Trilissera sprzed dziewięćdziesięciu pięciu lat.

Wydział, który prowadził nielegałów

W strukturze KGB program nielegałów prowadził Zarząd „S” (od słowa *specjalny*), najtajniejsza komórka jednej z najtajniejszych organizacji świata. To Zarząd „S” budował legendy, dobierał kandydatów, szkolił ich, plasował na Zachodzie i utrzymywał z nimi łączność. Po rozpadzie ZSRR funkcję tę przejęła SWR, gdzie odpowiednik Zarządu „S” istnieje do dziś. Archiwum tej komórki nigdy nie zostało otwarte; wiedza o niej pochodzi z relacji nielicznych dezerterów, z odtajnionych akt zachodnich służb oraz z notatek Wasilija Mitrochina, archiwisty KGB, który przez lata potajemnie kopiował dokumenty i wywiózł je na Zachód.

Dla naszego tematu, łączności bezosobowej, jedno spostrzeżenie: im głębiej ukryty był agent, tym bardziej potrzebował łączności, która nie wymagała kontaktu. Nielegał nie mógł po prostu wejść do ambasady. Nie mógł zadzwonić z prośbą o instrukcje. Cała jego wartość polegała na tym, że nic go nie łączyło z Moskwą, a to oznaczało, że każdy przekaz informacji czy pieniędzy musiał się odbywać w sposób, który tego braku powiązania nie niszczył. Łączność bezosobowa była więc nie dodatkiem do programu nielegałów, lecz jego warunkiem koniecznym.

Cena, jaką płacili ludzie

Walker konsekwentnie pokazuje drugą stronę tego kultu: koszt ludzki. Nielegałowie i ich rodziny płacili za tę służbę cenę, której „zwykli ludzie nigdy nie pojmą”, słowa, którymi rosyjska telewizja w 2024 roku opisała rodzinę Dulcewów. Dzieci wychowywane w przekonaniu, że są kimś innym, niż są. Małżeństwa zawierane na polecenie Centrali. Całe dekady życia w kłamstwie. Ten wątek, psychiczna trauma fundowana najbliższym, wraca w Części II, gdy opisujemy współczesne sprawy, bo pokazuje, że mimo całej technologicznej zmiany ludzki mechanizm pozostał ten sam.

Dla strony defensywnej ma to praktyczne znaczenie. Ludzie żyjący pod obcą tożsamością latami dźwigają obciążenie, które czasem przebija na powierzchnię: w drobnych niespójnościach biografii, w unikaniu fotografii, w nadmiernie gładkiej, „wyuczonej” historii życia. Rozdział 16 wróci do tych sygnałów jako do wskaźników rozpoznania.

Wniosek

Program nielegałów wyrósł z kultury konspiracji starszej niż samo państwo radzieckie i przetrwał wszystkie jego przemiany. Łączność bezosobowa była jego technicznym sercem, bo bez niej najgłębiej ukryty agent byłby bezużyteczny, nie mógłby ani odebrać instrukcji, ani przekazać zdobyczy. Zapamiętajmy tę zależność: głębokość przykrycia i potrzeba łączności bezosobowej rosną razem. W Części II zobaczymy, że gdy w erze cyfrowej klasyczna łączność bezosobowa stała się zbyt ryzykowna, przeciwnik nie porzucił samej zasady rozdzielania ludzi, przeniósł ją do sieci.

Rozdział 2a. Motywacje: dlaczego ludzie podejmują współpracę

Zrozumienie, dlaczego ludzie zdradzają lub dają się zwerbować, jest dla obrony równie ważne jak zrozumienie technik. Bo to motywacja jest punktem, w który uderza werbownik i punktem, który obrona może chronić.

Model MICE

Klasyczny model opisujący motywacje osób współpracujących z obcym wywiadem streszcza akronim MICE: *Money* (pieniądze), *Ideology* (ideologia), *Coercion/Compromise* (przymus, szantaż), *Ego*. Szwedzka analiza siedemdziesięciu wyroków za szpiegostwo w Europie z lat 2008–2024 potwierdziła, że model ten pozostaje trafny: w większości spraw (blisko 60 procent) w grę wchodziła korzyść finansowa, choć rzadko w izolacji od innych czynników.

Pieniądze. Najczęstszy i najbardziej uniwersalny motyw. W modelu jednorazowym jest wręcz jedynym, jaki werbownik oferuje: kilka tysięcy euro w kryptowalucie za zadanie. Odbiorcami są ludzie w trudnej sytuacji materialnej, zadłużeni, bezrobotni, migranci bez stabilnego dochodu. Dla obrony wniosek jest praktyczny: nagła, niewyjaśniona zmiana sytuacji finansowej pracownika, zarówno pogorszenie (podatność), jak i poprawa (możliwa zapłata), jest sygnałem wartym odnotowania w ramach modelu insider risk.

Ideologia. Historycznie napędzała najgroźniejszych agentów, tych, którzy zdradzali z przekonania, nie dla pieniędzy. W kontekście europejskim po 2022 roku ideologia bywa czynnikiem w sprawach osób o sympatiach prorosyjskich, choć w modelu jednorazowym gra mniejszą rolę niż desperacja finansowa. Osobną kategorią jest radykalizacja młodych ludzi w sieci, ABW i inne służby wskazują na nią jako na rosnący wektor.

Przymus i szantaż. Werbunek przez uwikłanie. Faza „testu" w cyklu werbunkowym (rozdz. 15) jest w istocie mechanizmem budowania dźwigni szantażu: gdy człowiek wykona pierwsze „niewinne" zadanie, staje się podatny na presję „już to zrobiłeś, teraz zrób więcej, bo inaczej…". Dla obrony to argument, by przechwytywać werbunek jak najwcześniej, przed fazą, w której zapłata zamienia się w haczyk.

Ego. Potrzeba uznania, poczucie krzywdy, chęć udowodnienia własnej wartości. Bywa, że agent działa, bo czuje się niedoceniony w miejscu pracy albo szuka poczucia ważności. Szwedzka analiza odnotowała, że rozczarowanie i uraza występowały w wielu sprawach.

Dlaczego to ma znaczenie dla obrony

Model MICE mówi obronie, gdzie jest słaby punkt organizacji: nie w murach, lecz w ludziach pod presją. Kultura, w której pracownik w kłopotach finansowych lub osobistych ma gdzie się zwrócić, w której zgłoszenie próby werbunku spotyka się ze wsparciem, a nie z podejrzeniem i w której nikt nie jest zostawiony sam z szantażem, jest realną barierą werbunkową. Twarda ochrona techniczna nie chroni przed człowiekiem,

którego ktoś złamał; chroni przed tym dobra kultura bezpieczeństwa i wsparcia. To dlatego model insider risk (rozdz. 17, Lista kontrolna C) kładzie nacisk na wsparcie i poufność, nie na inwigilację własnych ludzi.

Nowa motywacja: nieświadomość

Model jednorazowy dodał do MICE czynnik, którego klasyczny model nie przewidywał: **nieświadomość**. Znaczna część współczesnych wykonawców nie wie, dla kogo pracuje. Werbownik podszywa się pod zwykłego zleceniodawcę, kontakt idzie przez pośredników, słowo „Rosja” nigdy nie pada. Człowiek myśli, że wykonuje szemraną, ale „zwykłą” fuchę. Ta nieświadomość jest celowo wbudowana w model: daje mocodawcy zaprzeczalność, a wykonawcy złudne poczucie, że „nic wielkiego nie robi”. Dla obrony to argument za kampaniami uświadamiającymi (rozdz. 23): jeśli ludzie wiedzą, że „łatwa praca z Telegrama” to prawdopodobnie werbunek obcego wywiadu, nieświadomość przestaje działać jako osłona.

Rozdział 3. Anatomia klasycznej martwej skrzynki, spojrzenie z perspektywy śledczego

Ten rozdział celowo napisany jest z jednej perspektywy: śledczego, który *znalazł* skrzynkę albo próbuje ją znaleźć. Nie opisujemy, jak ją założyć. Opisujemy, jak wygląda i jak się zdradza, bo to jest wiedza, którą realnie posługuje się kontrwywiad i ochrona.

Co śledczy w ogóle szuka

Z punktu widzenia osoby chroniącej obiekt martwa skrzynka to nie jest „tajny schowek" w hollywoodzkim sensie. To zwykły, niepozorny element otoczenia, któremu ktoś nadał funkcję. Dlatego śledczy nie szuka „czegoś dziwnego", szuka **czegoś zwykłego, co znalazło się nie tam, gdzie powinno, albo zachowuje się nie tak, jak powinno**. Przedmiot pozostawiony w miejscu, w którym nikt niczego nie zostawia. Osoba, która zatrzymuje się na moment tam, gdzie nie ma powodu się zatrzymywać. Powtarzalność w miejscu, które powinno być przypadkowe.

Ta zmiana perspektywy jest fundamentem całej części szkoleniowej. Ochroniarz G4S patrolujący teren nie wykryje skrzynki, jeśli będzie szukał „szpiega". Wykryje ją, jeśli będzie znał normalny rytm swojego obiektu na tyle dobrze, by zauważyć odstępstwo. Anomalia na tle znanej normy, to jest narzędzie.

Trzy elementy, które musi powiązać śledczy

Klasyczna operacja łączności bezosobowej składała się, z grubsza, z trzech elementów: **miejsca**, **przedmiotu** i **sygnału**. Dla strony ofensywnej każdy z nich był starannie ukrywany. Dla strony defensywnej każdy z nich jest punktem zaczepienia.

Miejsce. Śledczego interesuje nie tyle sam schowek, ile *logika ruchu wokół niego*. Kto ma powód, by się tam znaleźć? Czy dana osoba pojawia się tam zgodnie z tą logiką, czy wbrew niej? Historyczne wpadki brały się często stąd, że obserwacja ustaliła, iż podejrzany odwiedza miejsce, do którego „nie miał po co" chodzić.

Przedmiot. Przesyłka miała wyglądać niewinnie i właśnie ta wymuszona niewinność bywa tropem. Przedmiot zbyt czysty, zbyt nowy, zbyt starannie umieszczony w miejscu, gdzie rzeczy trafiają przypadkowo, kłóci się z otoczeniem. Dla ochrony obiektu praktyczna zasada brzmi: podejrzanego przedmiotu się nie otwiera i nie przemieszcza, zabezpiecza się miejsce i wzywa właściwe służby (rozdział 17 i moduł G4S rozwijają tę procedurę).

Sygnał. System sygnałów istniał, żeby strony nie musiały się komunikować wprost. Nie podajemy, jak go budować. Z perspektywy defensywnej wystarczy wiedzieć, że *istnieje* i że przejawia się jako powtarzalny, z pozoru bezsensowny znak w przestrzeni: oznaczenie, przedmiot, ślad, który pojawia się i znika w rytmie

skorelowanym z czyimś zachowaniem. Nietypowe, powtarzalne oznaczenia w otoczeniu obiektu chronionego są wskaźnikiem, który warto odnotowywać.

> **SYGNAŁ OSTRZEGAWCZY.** Powtarzalność w miejscu, które z natury powinno być przypadkowe, jest jednym z najsilniejszych wskaźników. Pojedyncze zdarzenie niczego nie dowodzi. Ten sam nietypowy przedmiot, ślad albo osoba pojawiające się cyklicznie w tym samym punkcie, to jest to, co odnotowuje się w dzienniku i zgłasza.

> **UWAGA OPSEC.** Zwróćmy uwagę, czego w tym rozdziale nie ma: ani jednej wskazówki, jak dobrać miejsce, jak zamaskować przedmiot, jak ustawić sygnał tak, by nie wpaść. To nie jest przeoczenie, to jest linia, przy której opracowanie się zatrzymuje. Wszystko powyżej służy rozpoznaniu, nie wykonaniu.

Dlaczego akurat ta perspektywa jest przydatna w 2026 roku

Można zapytać: skoro klasyczne skrzynki wychodzą z użycia (Część II), po co uczyć się je rozpoznawać? Z dwóch powodów. Po pierwsze, nie wyszły z użycia całkowicie, nadal pojawiają się w operacjach, zwłaszcza przy przekazywaniu pieniędzy i sprzętu w siatkach, gdzie strony nie mogą sobie ufać. Po drugie i ważniejsze: *sposób myślenia* wyćwiczony na klasycznej skrzynce, szukanie anomalii na tle normy, powiązywanie rozdzielonych elementów, nieufność wobec „wymuszonej niewinności", jest dokładnie tym samym sposobem myślenia, którym rozpoznaje się współczesnego agenta jednorazowego prowadzącego rozpoznanie obiektu albo nadającego zapalającą paczkę. Narzędzie poznawcze jest przenaszalne, nawet jeśli technologia się zmienia.

Rozdział 4. Cztery klasyczne sprawy

Historia zna dziesiątki spraw łączności bezosobowej. Wybieramy cztery, bo każda uczy czego innego i każda ma bezpośredni odpowiednik we współczesnych rozdziałach. Wszystkie opisujemy z perspektywy tego, *jak zostały wykryte*, bo to jest defensywnie użyteczna część.

Rudolf Abel (Wiliam Fisher), nielegał wzorcowy i jego upadek

Człowiek znany na Zachodzie jako Rudolf Abel, a naprawdę Wiliam Fisher, był przez lata modelowym nielegałem KGB w Stanach Zjednoczonych. Jego sprawa, opisana szeroko przez Walkera, stała się w 1957 roku momentem, w którym świat po raz pierwszy publicznie dowiedział się o istnieniu programu nielegałów. Fisher nie wpadł jednak dzięki genialnej pracy analitycznej kontrwywiadu, lecz dlatego, że zdradził go jego własny współpracownik, Reino Häyhänen, alkoholik, którego Centrala chciała odwołać i który, przeczuwając swój los, przeszedł na stronę Amerykanów.

Nauka z tej sprawy jest ponadczasowa: **najsłabszym ogniwem tajnej operacji jest człowiek, nie technika.** Cała architektura łączności bezosobowej Fishera była bez zarzutu. Nie uratowała go, bo nie ochroni żaden system łączności, jeśli osoba wtajemniczona postanowi mówić. W Części II zobaczymy dokładnie ten sam mechanizm w sprawie Aleksandra Potiejewa, którego zdrada rozłożyła całą amerykańską siatkę nielegałów w 2010 roku.

Siatka z Portland, codzienność jako kamuflaż

Tak zwana Portland Spy Ring, rozbita w Wielkiej Brytanii w 1961 roku, pokazała, jak nielegałowie wtapiali się w zwyczajne życie. Para występująca jako Peter i Helen Kroger prowadziła z pozoru nudną egzystencję antykwariuszy książek; w rzeczywistości byli doświadczonymi agentami (Morris i Lona Cohen), a ich dom służył jako węzeł łączności radiowej i przekazu. Wpadli, gdy trop od zaniepokojonego informatora doprowadził brytyjski kontrwywiad do jednego z ogniw siatki, a systematyczna obserwacja rozplotła resztę.

Nauka: **normalność jest kamuflażem, ale normalność da się prześwietlić.** To, co czyniło Krogerów niewidzialnymi, nijakość, przewidywalność, brak cech szczególnych, jest tym samym, co dziś każe zwracać uwagę na „szarą myszkę", której biografia jest podejrzanie gładka. Walker celowo przywołuje reakcję sąsiadów Dulcewów w Słowenii: „to byli zwykli, mili ludzie, nie ma mowy, żeby byli szpiegami". Ta reakcja jest regułą, nie wyjątkiem i sama w sobie jest wskazówką.

Robert Hanssen, kret i łączność bezosobowa doprowadzona do perfekcji

Robert Hanssen, agent FBI szpiegujący dla Moskwy przez ponad dwie dekady, jest w naszym kontekście przypadkiem szczególnym: to Amerykanin sprzedający tajemnice Rosjanom, a nie nielegał, ale jego łączność z Moskwą była podręcznikowym przykładem systemu bezosobowego. Hanssen posunął zasadę rozdzielenia

tożsamości do skrajności, dbał, by prowadzący go oficerowie nie znali nawet jego nazwiska. To go przez lata chroniło.

A jednak wpadł. I znów nie dzięki złamaniu jego systemu łączności, lecz dlatego, że amerykański wywiad pozyskał od rosyjskiego źródła akta, które pozwoliły zidentyfikować kreta. Dopiero mając nazwisko, FBI zorganizowało obserwację i zatrzymało go w 2001 roku w momencie obsługi skrzynki. Kolejność jest tu pouczająca: **najpierw wywiad ludzki wskazał człowieka, dopiero potem obserwacja domknęła sprawę dowodowo.** Sam mechanizm łączności bezosobowej okazał się nie do złamania „od zewnątrz", złamano go „od środka".

Ghost Stories, dekada obserwacji i zdrada od wewnątrz

Operacja FBI o kryptonimie Ghost Stories, zakończona w czerwcu 2010 roku aresztowaniem dziesięciorga rosyjskich nielegałów (wśród nich Andrieja Biezrukowa i Jeleny Wawiłowej, występujących jako Donald Heathfield i Tracey Ann Foley, oraz Anny Chapman), jest zwornikiem między Częścią I a Częścią II. FBI śledziło tę siatkę przez blisko dekadę, podsłuchiwało, obserwowało, przeszukiwało. A mimo to momentem, który przesądził, była zdrada: pułkownik SWR Aleksandr Potiejew, odpowiedzialny za amerykański kierunek Zarządu „S", od lat informował Amerykanów. To on wydał całą siatkę.

> **RAMKA FAKTOGRAFICZNA: Ghost Stories.** Czerwiec 2010: FBI zatrzymuje dziesięcioro nielegałów SWR w USA. Kilka tygodni później dochodzi do wymiany na lotnisku w Wiedniu, Rosjanie odzyskują nielegałów, Zachód m.in. Siergieja Skripala. Siatka została rozpracowana dzięki wieloletniej obserwacji, ale wydana przez dezertera Potiejewa. Michaił Wasienkow (jako „Juan Lazaro"), najdłużej działający z tej grupy, do 2004 roku ograniczał aktywność do rocznego odbioru gotówki od prowadzącego.

Nauka podwójna. Po pierwsze, **cierpliwość działa**: dekada obserwacji zbudowała obraz, którego pojedynczy patrol nigdy by nie zobaczył. Po drugie, **ludzka zdrada pozostaje decydująca**: nawet najlepsza obserwacja potrzebowała punktu zaczepienia od wewnątrz. Obie nauki wracają w Części II, z tą różnicą, że współczesne siatki proxy dostarczają punktów zaczepienia znacznie więcej, bo ich wykonawcy zostawiają cyfrowe ślady, o których nielegałom się nie śniło.

Wspólny mianownik czterech spraw

We wszystkich czterech przypadkach system łączności bezosobowej sam w sobie okazał się bardzo trudny do złamania „od zewnątrz". To, co go pokonało, było zawsze jedną z dwóch rzeczy: **człowiek, który przeszedł na drugą stronę**, albo **cierpliwa, długotrwała obserwacja**, która czekała, aż operacja sama popełni błąd. Zapamiętajmy to, bo Część II pokaże trzecią, nową dźwignię, której w czasach Fishera i Krogerów nie było: **cyfrowy ślad**, który dziś sam wskazuje człowieka, zanim jeszcze ktokolwiek zdradzi.

Rozdział 4a. Więcej z historii łączności bezosobowej

Cztery sprawy z rozdziału 4 nie wyczerpują lekcji, jakich dostarcza historia. Ten rozdział dodaje kilka wątków, które wzbogacają obraz i mają współczesne odpowiedniki.

Archiwum Mitrochina, wartość jednego człowieka wewnątrz

Wasilij Mitrochin był archiwistą KGB, który przez lata, dzień po dniu, potajemnie kopiował akta z archiwum Zarządu, aż do przejścia na emeryturę w 1984 roku. Tysiące stron jego notatek, wywiezionych później na Zachód i udostępnionych w archiwum w Cambridge, stały się jednym z najcenniejszych źródeł wiedzy o radzieckim programie nielegałów, w tym o łączności bezosobowej. Sam Walker wielokrotnie korzysta z tego materiału.

Lekcja Mitrochina jest tą samą, co lekcja Fishera i Ghost Stories, tyle że widziana od drugiej strony: **jeden zdeterminowany człowiek wewnątrz systemu wart jest więcej niż lata pracy operacyjnej od zewnątrz.** Dla współczesnego kontrwywiadu oznacza to, że najcenniejsze wskazówki wciąż pochodzą od ludzi, dezerterów, informatorów, a dziś także od wykonawców siatek proxy, którzy postanawiają współpracować. Dla obrony organizacji przekłada się to na wartość każdego pracownika gotowego zgłosić to, co widzi.

Kult nielegała i jego cena

Walker konsekwentnie pokazuje, że program nielegałów otaczał w Rosji niemal religijny kult, od pomnika fikcyjnego Stirlitza po osobiste powitanie powracających agentów przez Putina na płycie lotniska. Ten kult jest częścią mechanizmu: podtrzymuje gotowość ludzi do poświęcenia dekad życia i tożsamości. Ale ma też drugą stronę, traumę fundowaną rodzinom, dzieciom wychowywanym w kłamstwie, małżeństwom zawieranym na rozkaz. Ta ludzka cena bywa źródłem pęknięć: napięć, niespójności, drobnych błędów, które strona defensywna potrafi dostrzec.

Ciągłość między epokami

Najważniejszą lekcją całej historii jest ciągłość. Metody się zmieniają, od radia i skrzynki po Telegram i kryptowaluty, ale ludzki mechanizm pozostaje ten sam: potrzeba przekazania czegoś bez zdradzenia powiązania, potrzeba motywacji do zdrady lub współpracy, słabość ludzka jako punkt wejścia i punkt wyjścia. Dlatego opracowanie zaczyna się od historii: nie z powodu nostalgii, lecz dlatego, że wzorce sprzed dekad wracają w nowych przebraniach, a kto je rozpoznaje w przeszłości, rozpozna je i dziś.

Rozdział 5. Dlaczego systemy łączności się sypały

Zbierzmy nauki z rozdziału 4 w spójny model, bo posłuży on jako pomost do współczesności. Klasyczne systemy łączności bezosobowej, mimo dekad doskonalenia, sypały się z pięciu powtarzalnych powodów.

Powód pierwszy: zdrada. Najczęstszy i najskuteczniejszy. Człowiek wtajemniczony, współpracownik, oficer prowadzący, archiwista, przechodzi na drugą stronę i wydaje siatkę. Häyhänen wydał Fishera. Potiejew wydał siatkę Ghost Stories. Mitrochin wyniósł archiwum, które przez dekady zasilało zachodnie służby. Żaden system techniczny nie chroni przed człowiekiem, który postanawia mówić.

Powód drugi: obserwacja skumulowana. Pojedynczy epizod niczego nie dowodzi, ale setki godzin obserwacji budują wzór. Kontrwywiad, który cierpliwie dokumentuje ruch podejrzanego, prędzej czy później uchwyci moment, w którym „niewinne" zachowanie przestaje dać się wytłumaczyć niewinnie.

Powód trzeci: błąd rzemieślniczy. Zmęczenie, rutyna, pośpiech. Agent, który przez lata robi to samo, popełnia w końcu drobny błąd, powtarza trasę, wraca po coś, zostawia ślad. Historia wywiadu to w dużej mierze historia takich drobnych błędów.

Powód czwarty: załamanie kontekstu. Legenda trzyma się, dopóki nikt jej nie prześwietla. Gdy zmienia się kontekst, wybucha wojna, służby zaczynają masowo weryfikować cudzoziemców danej narodowości, biografia, która wcześniej nie budziła pytań, nagle zaczyna nie pasować. Zobaczymy w Części II, że inwazja 2022 roku wywołała dokładnie takie masowe załamanie kontekstu dla rosyjskich nielegałów w Europie.

Powód piąty, nowy: cyfrowy ślad. Tego powodu w czasach Fishera nie było. Powszechny monitoring, dane lokalizacyjne z telefonów, rejestry przekroczeń granic, rozpoznawanie twarzy, wycieki baz danych, płatności zostawiające ślad, wszystko to sprawiło, że rozdzielenie dwojga ludzi, którzy nigdy się nie spotkali, przestało wystarczać. Dziś system nie musi ich „spotkać", by ich powiązać. Wystarczy, że oboje zostawili ślady, które da się zestawić.

To piąty powód przesądził o zmierzchu klasycznego nielegała i klasycznej skrzynki i to on tłumaczy, dlaczego przeciwnik przeszedł do modelu, który opisuje Część II. Jeśli zbudowanie wiarygodnej legendy, która przejdzie kontrolę biometryczną, zajmuje dziś lata i i tak grozi dekonspiracją przy pierwszym poważnym prześwietleniu, to taniej i „bezpieczniej" jest wysłać w teren kogoś, kto niczego nie udaje, bo jest tym, kim jest i po prostu wykona jedno zadanie, za które zapłaci mu się w kryptowalucie, a potem zniknie z jego życia. Tak rodzi się agent jednorazowy.

Podsumowanie Części I

Łączność bezosobowa była technicznym sercem programu nielegałów: pozwalała najgłębiej ukrytemu agentowi utrzymać kontakt z Centralą bez niszczenia tego, co czyniło go cennym, braku powiązań z Moskwą.

Realizowała trzy funkcje: rozdzielenie ludzi, zaprzeczalność, odporność na obserwację. Przez dekady była niemal nie do złamania od zewnątrz. Pokonywały ją zdrada i cierpliwa obserwacja, a w erze cyfrowej doszedł trzeci, decydujący czynnik: ślad danych. To on uczynił klasyczny model tak ryzykownym, że przeciwnik zaczął go zastępować. Jak, o tym Część II.

CZĘŚĆ II. AKTUALIZACJA PO 2022, OD NIELEGAŁA DO AGENTA JEDNORAZOWEGO

Rozdział 6. Cezura lutego 2022 i załamanie rezydentur legalnych

Dzień, który przemeblował rosyjski wywiad w Europie

24 lutego 2022 roku Władimir Putin rozkazał pełnoskalową inwazję na Ukrainę. Dla naszego tematu ta data jest cezurą nie tylko militarną i polityczną, lecz także wywiadowczą. Walker w posłowiu do swojej książki opisuje inwazję jako „kolosalną porażkę wywiadu": pieniądze na budowę siatki zwolenników w Ukrainie rozkradziono, a otoczenie Putina uwierzyło we własną propagandę, że Ukraińcy powitają Rosjan. Ale skutki uderzyły również w rosyjski aparat wywiadowczy w całej Europie i to w sposób, który wprost tłumaczy późniejszą falę sabotażu.

W odpowiedzi na inwazję państwa zachodnie przeprowadziły największą od dekad wspólną operację wydalenia rosyjskich dyplomatów. W ciągu miesięcy setki oficerów działających pod przykryciem dyplomatycznym, czyli rdzeń rezydentur legalnych SWR i GRU, musiały wrócić do Moskwy. Jak ujmuje to Walker, „nagle SWR i GRU straciły wszelkie zdolności". Zamknięto połączenia lotnicze, zaostrzono politykę wizową, „zwykłemu" obywatelowi rosyjskiemu odebrano łatwość podróżowania na Zachód, z której przez dwie dekady korzystały setki tysięcy ludzi i z której korzystali też agenci podający się za turystów.

Dlaczego to wywołało falę sabotażu

Ta zmiana ma kluczowe znaczenie dla zrozumienia wszystkiego, co nastąpiło potem. Rosyjski wywiad przez lata realizował operacje w Europie głównie dwiema drogami: przez oficerów pod przykryciem dyplomatycznym oraz przez „turystów" z rosyjskimi paszportami, jak dwaj oficerowie jednostki 29155, którzy w 2018 roku podali się za „sprzedawców witamin" i próbowali otruć Siergieja Skripala w Salisbury. Po 2022 roku obie te drogi zostały w dużej mierze zamknięte. Wydalono dyplomatów; rosyjski paszport przestał być kluczem do Europy.

Moskwa stanęła więc przed problemem: jak prowadzić operacje w Europie bez oficerów w ambasadach i bez możliwości wysyłania własnych ludzi jako turystów? Odpowiedzią stały się dwie rzeczy, które opisuje reszta tej części. Po pierwsze, **powrót do klasycznych nielegałów** z tożsamością państw trzecich (rozdział 7). Po drugie i na masową skalę, **outsourcing operacji do lokalnych pośredników**, ludzi już obecnych na miejscu, werbowanych zdalnie, jednorazowych (rozdziały 8–10). To drugie rozwiązanie okazało się tańsze, szybsze i, z punktu widzenia Moskwy, całkowicie zaprzeczalne.

> **RAMKA FAKTOGRAFICZNA: skala wydaleń i skutek.** Po lutym 2022 państwa zachodnie wydaliły setki rosyjskich oficerów działających pod przykryciem dyplomatycznym. Efektem była, jak pisze Walker, utrata bieżących zdolności rezydentur legalnych SWR i GRU w Europie oraz zwrot Moskwy ku nielegałom i pośrednikom. Ośrodki analityczne (m.in. Carnegie Europe, 2026) odnotowały następnie

> „czterokrotny wzrost” liczby rosyjskich operacji sabotażowych w Europie od 2024 roku.

Nowa geografia zagrożenia

Wraz z tą zmianą przesunął się też środek ciężkości zagrożenia. Klasyczny nielegał celował w tajemnice, plany, technologie, dostęp do decydentów. Nowa fala jest inna: jej celem jest przede wszystkim **zakłócenie i zastraszenie**. Podpalenia magazynów z pomocą dla Ukrainy, rozpoznanie i sabotaż infrastruktury kolejowej, przesyłki zapalające w łańcuchu kurierskim, rozpoznanie obiektów wojskowych i baz, przez które płynie wsparcie dla Kijowa. Cel nie jest już wyłącznie wywiadowczy, jest paramilitarny. To wojna hybrydowa prowadzona rękami ludzi, którzy często nie wiedzą nawet, dla kogo naprawdę pracują.

Dla obrońcy, czy to placówki dyplomatycznej, czy węzła logistycznego, czy odcinka kolei, oznacza to fundamentalną zmianę profilu przeciwnika. Nie stoi naprzeciw nam już wyłącznie wyszkolony oficer o nienagannej legendzie. Coraz częściej stoi zdesperowany finansowo miejscowy, zwerbowany trzy tygodnie temu przez czat, który wykona jedno zadanie za kilka tysięcy euro w kryptowalucie. To zmienia wszystko: wskaźniki, metody wykrywania, a nawet to, kto jest potencjalnym zagrożeniem wewnątrz organizacji.

Rozdział 6a. Szersze tło: środowisko bezpieczeństwa po 2022 roku

Zanim przejdziemy do szczegółów siatek proxy, warto umieścić je w szerszym kontekście zmian w środowisku bezpieczeństwa, jakie przyniósł okres po lutym 2022. Rosyjska kampania hybrydowa w Europie nie jest zjawiskiem izolowanym, jest elementem szerszej rekonfiguracji, w której wojna, wywiad i sabotaż splatają się ściślej niż w jakimkolwiek momencie od zakończenia zimnej wojny.

Wojna, która nie mieści się w dawnych kategoriach

Pełnoskalowa wojna na Ukrainie zmieniła sposób, w jaki myślimy o granicy między pokojem a wojną. Klasyczny podział, albo trwa konflikt zbrojny, albo panuje pokój, okazał się niewystarczający. Między tymi stanami rozciąga się dziś szeroka „szara strefa": przestrzeń działań, które nie są otwartą wojną, ale też nie są pokojem. Sabotaż infrastruktury, podpalenia magazynów, przesyłki zapalające, naruszenia przestrzeni powietrznej przez drony, uszkodzenia kabli podmorskich, cyberataki, kampanie dezinformacyjne, instrumentalne wykorzystywanie migracji, wszystko to należy do repertuaru szarej strefy. Amerykańska doroczna ocena zagrożeń z 2026 roku wprost wymienia „cyberataki, dezinformację i operacje wpływu, manipulację rynkiem energii, zastraszanie militarne oraz sabotaż" jako narzędzia rosyjskiej gry w szarej strefie.

Dla obrońcy oznacza to fundamentalną zmianę. Nie wystarcza już myślenie w kategoriach „czy jesteśmy na wojnie", trzeba założyć, że pewien poziom wrogich działań trwa stale, nawet jeśli formalnie panuje pokój. Chroniony obiekt w Polsce w 2026 roku funkcjonuje w środowisku, w którym akt sabotażu nie jest scenariuszem hipotetycznym, lecz udokumentowaną rzeczywistością (Mika, Puławy). Ta zmiana świadomości jest punktem wyjścia dla całej filozofii obrony przedstawionej w tym opracowaniu.

Nowe fronty, ta sama logika

Okres po 2022 roku przyniósł nie tylko intensyfikację wojny na Ukrainie, ale i szereg dodatkowych ognisk napięć i konfliktów w skali globalnej, które pośrednio wpływają na europejskie środowisko bezpieczeństwa. Rosja zacieśniła współpracę z państwami, które amerykańska ocena zagrożeń określa jako partnerów w konfrontacji z Zachodem. Konflikty i napięcia w innych regionach świata angażują uwagę i zasoby zachodnich służb, tworząc, z punktu widzenia Moskwy, okazję do działania w Europie przy relatywnie mniejszym ryzyku. Wojna stała się, jak ujmują to analitycy, nie tylko instrumentem polityki zagranicznej, lecz „mechanizmem rządzenia" podtrzymującym reżim wewnętrznie.

Dla naszego tematu istotne jest jedno: mimo mnożenia się frontów logika rosyjskich operacji w Europie pozostaje ta sama. Cel to osłabienie wsparcia dla Ukrainy, rozbicie spójności Zachodu i zasianie poczucia niepewności. Narzędziem jest sabotaż rękami pośredników. A słabym punktem tego narzędzia, jak pokazuje

cała Część II, pozostaje ślad, który każdy wykonawca zostawia. Zmiana skali i geografii nie zmienia mechanizmu obrony.

Zbieżność rozpoznania i ataku

Najważniejszą jakościową zmianą po 2022 roku jest zacieranie się granicy między rozpoznaniem a atakiem. W dawnym modelu rozpoznanie było odrębną, wcześniejszą i łagodniejszą fazą, agent fotografował obiekt, a atak (jeśli następował) był osobnym przedsięwzięciem. Dziś te fazy się zlewają. Dron, który dziś rozpoznaje obiekt, jutro może przenieść ładunek, jak pokazał incydent z dronem wykrytym przy samolocie cargo na lotnisku Lipsk-Halle w sierpniu 2026 roku. Paczka, która dziś testuje trasę logistyczną z nadajnikiem GPS, jutro może zawierać ładunek zapalający, co pokazało zestawienie sprawy paczek z GPS (Stuttgart 2026) z kampanią paczek zapalających (2024).

Dla obrony wniosek jest jednoznaczny: rozpoznania nie wolno lekceważyć jako „tylko obserwacji". Każdy wykryty akt rozpoznania należy traktować jako wczesną fazę potencjalnego ataku i reagować odpowiednio. To założenie leży u podstaw modułu wykrywania wrogiego rozpoznania w Części III.

Dlaczego akurat teraz warto szkolić

Zbieg trzech okoliczności czyni obecny moment szczególnie właściwym dla inwestycji w szkolenie i odporność. Po pierwsze, zagrożenie jest realne i udokumentowane, nie hipotetyczne. Po drugie, przeciwnik przeszedł na model, który, mimo groźności, jest wykrywalny przez uważny personel, bo opiera się na amatorach zostawiających ślady. Po trzecie, państwa i służby przeszły od milczenia do jawnego ostrzegania, tworząc klimat, w którym czujność obywatela i pracownika jest oczekiwana i wspierana. Innymi słowy: zagrożenie jest poważne, obrona jest możliwa, a otoczenie sprzyja. To jest właściwy moment.

Rozdział 6b. Synergia, o której wszyscy zapomnieli

Stan na wrzesień 2026.

Wniosek stawiam od razu, bo to jest oś całej tej książki. Ostatnią dekadę branża bezpieczeństwa przespała na jednym łóżku z napisem cyber. Budżety, konferencje, etaty, uwaga zarządów, wszystko poszło w stronę zapór, SOC-ów i szkoleń z phishingu. I dobrze, że poszło, bo cyber jest realny. Problem w tym, że przeciwnik nigdy nie grał w jednym wymiarze, a my nauczyliśmy się patrzeć w jeden. Rosja po 2022 roku nie prowadzi w Europie kampanii cybernetycznej ani kampanii sabotażowej, ani kampanii werbunkowej. Prowadzi jedną kampanię, w której to wszystko jest połączone. I właśnie to połączenie, ta synergia, jest tym, czego większość organizacji nie widzi, bo każdy pilnuje swojego kawałka.

Jak wygląda pojedyncza operacja, gdy się jej przyjrzeć w całości

Weźmy podpalenie magazynu z pomocą dla Ukrainy, bo to jest sprawa udokumentowana wyrokiem, nie hipoteza. Londyn, Leyton, marzec 2024, cel to magazyn z pomocą i sprzętem Starlink. Rozłóżmy tę jedną operację na warstwy.

Warstwa cyfrowa: Dylan Earl kontaktuje się z Grupą Wagnera przez Telegram i tam zgłasza gotowość do misji. Rekrutacja wykonawców też idzie przez komunikatory. Warstwa finansowa: obietnica zapłaty, ludzie z desperacji i z chęci zysku. Warstwa fizyczna: właściwe podpalenie, milion funtów strat. Warstwa dowodowa, którą przeciwnik wytworzył sam: transmisja nagrania z podpalenia do zleceniodawcy, bo bez dowodu nie ma zapłaty. Do tego zwykłe ślady świata fizycznego, CCTV, kamery drogowe, zakup paliwa, DNA na nożu.

Teraz pytanie, które lubię zadawać na szkoleniach. Czyj to był problem. Działu IT, bo werbunek szedł przez Telegram. Ochrony fizycznej, bo palił się magazyn. HR, bo w grę wchodzili ludzie i ich motywacje. Kontrwywiadu, bo za wszystkim stało obce państwo. Odpowiedź brzmi: wszystkich naraz i nikogo z osobna. I to jest cała rzecz. Operacja była synergiczna, a obrona w większości firm jest posiekana na silosy, z których każdy widzi jedną warstwę i żaden nie widzi całości.

Dlaczego akurat teraz to boli

Oceniam, że przejście przeciwnika na model synergiczny nie było wyborem estetycznym, tylko wymuszeniem. Po wydaleniu dyplomatów i zamknięciu drogi turysty z rosyjskim paszportem Moskwa straciła wygodne, jednowymiarowe narzędzia. Nie mogła już wysłać oficera pod przykryciem ambasady ani agenta udającego turystę. Musiała złożyć operację z części, które są osobno legalne albo niewinne. Konto na Telegramie jest legalne. Przelew w krypto jest legalny. Paczka w DHL jest legalna. Człowiek robiący zdjęcia budynku nie łamie prawa. Dron kupiony w sklepie jest legalny. Dopiero złożenie tych części w całość daje sabotaż.

Przeciwnik nauczył się budować atak z klocków, z których każdy z osobna przechodzi przez każdy pojedynczy filtr.

To jest dokładnie ten sam mechanizm, który kiedyś dawała martwa skrzynka. Skrzynka rozdzielała ludzi w czasie i przestrzeni, żeby żaden pojedynczy moment nie zdradzał całości. Model synergiczny rozdziela operację na warstwy, żeby żaden pojedynczy filtr nie zobaczył całości. Zmienił się nośnik, została logika. I obrona, która patrzy warstwami, jest wobec tej logiki bezradna, tak jak kontrwywiad bez obserwacji był bezradny wobec dobrze zrobionej skrzynki.

Co to znaczy dla obrony, konkretnie

Skoro atak jest synergiczny, obrona też musi być. Nie chodzi o kolejny dział ani o nową platformę. Chodzi o to, żeby warstwy, które dziś patrzą osobno, zaczęły ze sobą rozmawiać.

Pokażę to na jednej sytuacji. Pracownik dostaje na Telegramie ofertę drobnej fuchy za zrobienie zdjęć bramy. To sygnał cyfrowy i personalny naraz. Tego samego tygodnia ochrona odnotowuje pod ogrodzeniem auto, które wraca. To sygnał fizyczny. Osobno każdy z tych sygnałów jest słaby. Zgłoszenie o dziwnej wiadomości ląduje w HR albo w IT i tam umiera. Notatka patrolu ląduje w dzienniku ochrony i tam umiera. Dopiero gdy ktoś położy te dwie rzeczy obok siebie, widać rozpoznanie obiektu w toku. Synergia w obronie to jest właśnie ten stół, na którym te dwie kartki leżą obok siebie i osoba, która ma prawo i nawyk je zestawić.

Oceniam, że dla większości organizacji to jest tańsza zmiana niż cokolwiek technicznego, bo nie wymaga kupowania, tylko przestawienia. Jeden kanał, do którego spływają sygnały ze wszystkich warstw. Jedna osoba albo mały zespół, który ma mandat je korelować. Rytm, w którym drobne anomalie z ochrony, z IT, z HR i z recepcji są okresowo zestawiane, a nie zamykane w osobnych szufladach. To nie jest rewolucja. To jest zszycie tego, co już mamy.

Gdzie jest pułapka

Uczciwie, bo obiecałem pisać też to, co osłabia moją tezę. Synergia w obronie ma dwa koszty, o których łatwo zapomnieć. Pierwszy to szum. Jeśli zaczniemy zbierać wszystko ze wszystkich warstw bez zasady wielu wskaźników i bez znajomości normy, utoniemy w sygnałach i przestaniemy widzieć te ważne. Korelacja bez dyscypliny to nie czujność, to hałas. Drugi koszt to prywatność i zaufanie. Zszywanie danych z HR, z IT i z ochrony łatwo zsuwa się w inwigilację własnych ludzi, a to niszczy dokładnie tę kulturę zgłaszania, na której cała obrona stoi. Granica jest cienka i nie udaję, że wiem, gdzie dokładnie leży w każdej firmie. Wiem tylko, że po jednej jej stronie jest odporność, a po drugiej organizacja, w której nikt już niczego nie zgłasza, bo wszyscy czują się obserwowani.

Czego nie wiem

Nie wiem, ile organizacji w Polsce ma dziś realny stół, na którym warstwy się spotykają, a ile ma go tylko na schemacie. Podejrzewam, że mniej, niż deklarują, ale tego nie zmierzyłem. Nie wiem, jak szybko przeciwnik pójdzie o krok dalej i zacznie synchronizować warstwy w czasie, na przykład łącząc cyberatak z fizycznym sabotażem w jednym oknie, żeby maksymalnie obciążyć reakcję. Widać zaczątki takiego myślenia w naruszeniach przestrzeni powietrznej i w incydentach na infrastrukturze, ale twardego, udokumentowanego przykładu pełnej synchronizacji na europejskim obiekcie nie mam i dlatego tego nie twierdzę.

Jedno mówię z przekonaniem, bo to jest sedno. Kto broni tylko cyber, przegapi operację, która wchodzi przez bramę. Kto broni tylko bramy, przegapi tę, która wchodzi przez czat. Przeciwnik już to zrozumiał. Pytanie brzmi, czy zrozumie to obrona, zanim nauczy jej tego kolejny magazyn albo kolejny tor.

Rozdział 7. Powrót klasycznych nielegałów: Czerkasow, Dulcewowie, Kołobowa

Choć środek ciężkości przesunął się ku pośrednikom, Moskwa nie porzuciła klasycznych nielegałów. Przeciwnie, jak pokazuje Walker i późniejsze sprawy, po wpadce siatki Ghost Stories z 2010 roku wyszkolono nowe pokolenie, które inwazja 2022 roku zaczęła wypłukiwać na powierzchnię. Trzy sprawy pokazują, jak ten model wygląda dziś i dlaczego coraz trudniej mu przetrwać.

Siergiej Czerkasow, nielegał zdemaskowany u progu celu

Siergiej Czerkasow działał pod tożsamością brazylijskiego naukowca Victora Mullera Ferreiry. Zbudował wiarygodną legendę, studia, w tym dyplom uczelni na Zachodzie i w 2022 roku zmierzał do stażu w Międzynarodowym Trybunale Karnym w Hadze. Termin nie był przypadkowy: trybunał miał właśnie rozpocząć badanie rosyjskich zbrodni wojennych w Ukrainie. Nielegał SWR u progu instytucji ścigającej jego mocodawców, trudno o wyraźniejszy obraz intencji.

Holendrzy go zdemaskowali i deportowali, zanim zdążył wejść do trybunału. Czerkasow trafił do Rosji okrężną drogą przez Brazylię, gdzie odsiadywał wyrok za fałszerstwo dokumentów. W 2026 roku, po odrzuceniu amerykańskiego wniosku o ekstradycję, sąd brazylijski orzekł jego deportację i wieloletni zakaz wjazdu. Sprawa Czerkasowa pokazuje wzór: nawet dobrze zbudowana legenda pęka dziś przy poważnej weryfikacji instytucjonalnej, a Zachód po 2022 roku weryfikuje cudzoziemców z określonym profilem znacznie uważniej.

> **RAMKA FAKTOGRAFICZNA: Siergiej Czerkasow.** Nielegał (przypisywany GRU/SWR) pod tożsamością Brazylijczyka Victora Mullera Ferreiry. Cel: staż w MTK w Hadze w 2022 r., w momencie otwarcia śledztwa ws. zbrodni rosyjskich w Ukrainie. Zdemaskowany i zawrócony przez Holandię; osadzony w Brazylii; w 2026 r. sąd brazylijski orzekł deportację i 30-letni zakaz wjazdu. USA bezskutecznie wnioskowały o ekstradycję.

Dulcewowie, nielegałowie „z podręcznika” i ich koniec

Sprawa Anny i Artioma Dulcewów jest najpełniejszą współczesną ilustracją klasycznego modelu i jego zmierzchu. Występowali jako Argentyńczycy: María Mayer, kuratorka galerii sztuki i Ludwig Gisch, przedsiębiorca IT. Osiedlili się w Słowenii, kraju małym, spokojnym, a przy tym położonym w strefie Schengen, co pozwalało poruszać się po Europie bez kontroli paszportowej. Wychowywali dwoje dzieci w przekonaniu, że są hiszpańskojęzycznymi katolikami z Ameryki Łacińskiej. Galeria i firma IT dawały pretekst do podróży: María jeździła na targi sztuki, Ludwig na branżowe konferencje, w tym, jak odnotowuje Walker, na dużą konferencję branży cyberbezpieczeństwa w Niemczech.

W grudniu 2022 roku słoweńskie służby aresztowały parę w jednej z największych obław w historii kraju. Dzieci trafiły do rodzin zastępczych. Podczas przeszukania biura i domu znaleziono tak dużo gotówki, że jej przeliczenie zajęło godziny; w ukrytej przegródce lodówki leżały setki tysięcy euro. Informator ze służb powiedział Walkerowi, że para latami tkwiła w uśpieniu, a po inwazji na Ukrainę została „aktywowana" do bardziej ryzykownych zadań.

Zdemaskowanie zawdzięczamy w dużej mierze białemu wywiadowi. Christo Grozev, śledczy współpracujący z Bellingcat, ustalił prawdziwe tożsamości: María to Anna Dulcewa, urodzona w 1981 roku w Gorkim; Ludwig to Artiom Dulcew, rocznik ten sam. Punktem zaczepienia było zdjęcie twarzy Marii na stronie internetowej szkoły dzieci, mimo że para latami unikała fotografowania. Grozev zlecił przeszukanie rosyjskiej bazy paszportowej techniką rozpoznawania twarzy; korupcja w Rosji uczyniła takie bazy dostępnymi na czarnym rynku. W sierpniu 2024 roku Dulcewów objęto wielką wymianą więźniów na lotnisku w Ankarze; na płycie w Moskwie witał ich osobiście Putin. Dopiero w samolocie rodzice wyjaśnili dzieciom, że nie pochodzą z Argentyny.

> **SYGNAŁ OSTRZEGAWCZY: z tej sprawy.** Konsekwentne unikanie fotografii; „firma" z pretekstową, ubogą działalnością, służąca głównie jako uzasadnienie podróży; duże ilości gotówki bez pokrycia w widocznej działalności; podejrzanie gładka, mało konkretna biografia z odległego kraju, której nikt lokalnie nie potrafi zweryfikować. Reakcja otoczenia, „to niemożliwe, to zwykli, mili ludzie", jest regułą, nie kontrargumentem.

Olga Kołobowa, „Maria Adela" z Neapolu

Trzeci przypadek, również rozpracowany przez Grozeva, to Olga Kołobowa, występująca jako peruwiańska projektantka biżuterii Maria Adela Rivera, mieszkająca w Neapolu i utrzymująca kontakty z oficerami marynarek państw NATO. Grozev namierzył ją między innymi dzięki danym z mikroczipa jej kota, detal, który brzmi anegdotycznie, ale doskonale ilustruje istotę zmiany: w świecie gęstym od danych każdy ślad, nawet weterynaryjny, może stać się nitką, za którą rozplata się cała legenda.

Wspólny wniosek trzech spraw

Klasyczny nielegał nie zniknął, ale działa dziś w środowisku dla niego zabójczym. Rozpoznawanie twarzy, wycieki baz danych, OSINT, ślad cyfrowy dzieci i zwierząt, wzmożona po 2022 roku czujność instytucji, wszystko to sprawia, że legenda budowana latami pęka przy pierwszym poważnym prześwietleniu. Samo źródło Walkera w Moskwie przyznało w 2024 roku: „w erze sztucznej inteligencji i danych biometrycznych znacznie trudniej jest budować dla nowych nielegałów legendy, które przejdą przez kontrolę". A jednak to samo źródło dodało, że „zapotrzebowanie na nielegałów pozostaje ogromne", bo w decydującym momencie nadal potrzebny jest człowiek w terenie. To napięcie, rosnące zapotrzebowanie przy rosnącym ryzyku dekonspiracji, jest dokładnie tym, co pchnęło Moskwę ku modelowi jednorazowemu.

Rozdział 8. GRU, jednostka 29155 i przemysł sabotażu

Od pojedynczych operacji do systemu

Walker odnotowuje, że po 2010 roku GRU utworzyło jednostkę nielegałów organizujących „zabójstwa, zamachy bombowe i podpalenia w całej Europie". Jednostka ta, znana z numeru **29155**, nie posługiwała się latami budowanymi legendami, jej ludzie podawali się za rosyjskich turystów albo korzystali z paszportów byłych republik radzieckich. To ci sami ludzie, którzy w 2014 roku pojawili się w Czechach, by wysadzić skład amunicji we Vrběticach (uznany przez GRU za kanał przerzutu broni na Ukrainę), a cztery lata później otruli nowiczokiem Siergieja Skripala w Salisbury.

29155 jest ważne, bo stanowi pomost między starym a nowym modelem. To wciąż jednostka wysyłająca w teren własnych oficerów, ale już bez wieloletniej legendy, „na szybko", pod płytkim przykryciem turysty. Po 2022 roku, gdy rosyjski paszport przestał otwierać granice, ten model musiał ewoluować dalej: skoro nie można już wysłać własnego człowieka jako turysty, trzeba znaleźć kogoś, kto już jest na miejscu. Tak funkcja 29155, organizowanie sabotażu i dywersji za granicą, została w dużej mierze przekazana lokalnym pośrednikom, sterowanym zdalnie. Jednostka nie zniknęła; zmieniła sposób sięgania po wykonawców.

Przemysł, nie pojedyncze akcje

To, co obserwujemy w Europie od 2023 roku, najlepiej opisać słowem **przemysł**. Nie chodzi o pojedyncze, spektakularne operacje w rodzaju Salisbury, lecz o rozproszoną, ciągłą kampanię drobnych aktów: podpaleń, rozpoznania, prób sabotażu, przesyłek zapalających. Ośrodki analityczne mówią o czterokrotnym wzroście liczby rosyjskich operacji sabotażowych w Europie od 2024 roku. GLOBSEC i inni opisują to jako „przemysł crime-terror nexus", splot rosyjskich służb ze światem drobnej przestępczości, w którym państwo zamawia usługę, a wykonuje ją ktoś, kto normalnie zajmuje się czymś zupełnie innym.

Zmiana skali jest sama w sobie strategią. Pojedynczą operację Salisbury da się przypisać, potępić, ukarać wydaleniami. Rozproszoną kampanię setek drobnych incydentów, z których każdy z osobna jest „tylko" podpaleniem czy wandalizmem popełnionym przez miejscowego, znacznie trudniej przypisać państwu, jeszcze trudniej ukarać, a jej łączny efekt, poczucie ciągłego zagrożenia, nadwyrężenie służb, presja na osłabienie poparcia dla Ukrainy, jest dokładnie tym, o co Moskwie chodzi. Czeski kontrwywiad BIS ujął cel wprost: „osłabianie spójności zachodnich społeczeństw, szerzenie strachu i niepewności, podważanie zaufania obywateli do zdolności państwa do ich ochrony oraz zwiększanie presji na ograniczenie wsparcia dla Ukrainy".

Cele: logistyka wsparcia dla Ukrainy

Geografia celów nie jest przypadkowa. Kampania koncentruje się na infrastrukturze, przez którą płynie wsparcie dla Kijowa: magazyny pomocy, węzły logistyczne, linie kolejowe wiodące na wschód, lotniska cargo, zakłady zbrojeniowe, bazy, przez które przechodzi sprzęt. To wojna prowadzona na zapleczu wojny, próba przerwania lub choćby utrudnienia strumienia zaopatrzenia oraz zastraszenia społeczeństw, które ten strumień utrzymują.

Dla obrońcy oznacza to jasną wskazówkę co do tego, kto jest celem. Jeżeli chronisz obiekt związany z logistyką, energetyką, koleją, obronnością albo wsparciem dla Ukrainy, jesteś w kręgu zainteresowania tej kampanii, niezależnie od tego, jak „cywilny” wydaje się twój obiekt. Ta świadomość jest pierwszym krokiem obrony.

Rozdział 9. Werbunek przez Telegram, anatomia maszyny

To jest centralny rozdział całej Części II, bo opisuje mechanizm, który zastąpił klasyczną łączność bezosobową jako główny sposób sięgania po wykonawców. Rekonstruujemy go wyłącznie po to, by go rozpoznawać i tak jest napisany.

Ogłoszenie, od którego się zaczyna

Werbunek zaczyna się dziś nie od oficera prowadzącego na ławce w parku, lecz od ogłoszenia w komunikatorze. Schemat jest powtarzalny: „Łatwa praca. Dobre pieniądze. Napisz na Telegramie". Czasem przybiera formę półautomatycznego bota (śledczy opisywali konto działające jako „Privet Bot"), za którym stoi żywy rekruter. Kontakt zaczyna się od wyboru języka i lokalizacji, potem padają pytania weryfikujące: doświadczenie wojskowe, karalność, gotowość do „poważniejszych" zadań. Płatność, w kryptowalucie, „po wykonaniu".

Odbiorcami są przede wszystkim ludzie w trudnej sytuacji finansowej, często z przeszłością kryminalną, migranci, czasem bardzo młodzi ludzie zradykalizowani w sieci. Fińska SUPO, niemieckie BfV i BKA, czeska BIS zgodnie opisują ten sam profil: „osoby o wcześniejszej karalności i żyjące w trudnych warunkach". Najważniejsze: **wielu z nich nie wie, dla kogo naprawdę pracuje**. Kontakt idzie przez pośredników i tymczasowe konta, państwo pozostaje niewidoczne. To celowa konstrukcja: zapewnia zaprzeczalność mocodawcy i „niewinność" wykonawcy jednocześnie.

Sześć faz, model SUPO

Fińska służba bezpieczeństwa opisała cały cykl jako sześć faz. Przytaczamy je, bo stanowią kręgosłup części szkoleniowej (rozdział 15).

Faza 1, kontakt. Nagabywanie w mediach społecznościowych i komunikatorach, zwłaszcza na Telegramie. Cel: ludzie z potrzebą finansową lub sympatiami prorosyjskimi.

Faza 2, test. Drobne, z pozoru niewinne zadanie: rozwieszenie plakatów, zrobienie zdjęć, przewiezienie paczki. Służy sprawdzeniu, czy kandydat jest posłuszny i dyskretny, zanim powierzy mu się coś poważniejszego. To jest moment przejścia, pozornie błahy, w istocie decydujący.

Faza 3, eskalacja. Zadania rosną: obserwacja obiektów, podpalenie, wandalizm, w skrajnych przypadkach ładunek. Płatność rośnie razem z ryzykiem.

Faza 4, dowód wykonania. Wymóg nagrania. Działanie trzeba sfilmować, żeby dostać zapłatę. Ten wymóg, z pozoru banalny, jest jedną z największych słabości modelu z punktu widzenia wykonawcy: tworzy dowód przeciwko niemu i lokalizuje go w czasie i miejscu.

Faza 5, zatrzymanie. Zachodnie służby reagują szybko. Wykonawcy są zatrzymywani i stają przed sądem, nierzadko pod zarzutami działania na rzecz obcego państwa lub o charakterze terrorystycznym, zagrożonymi wieloletnim więzieniem.

Faza 6, konsekwencje. Rekrut jest „jednorazowy". Po zatrzymaniu nie dostaje żadnego wsparcia. Mocodawca znika. Zostaje sam z wyrokiem w obcym kraju.

> **RAMKA FAKTOGRAFICZNA: „agent do wyrzucenia".** Niemieckie służby (BKA, BND, BfV, BAMAD) uruchomiły 2 września 2025 r. wspólną kampanię informacyjną „Kein Wegwerf-Agent werden!" („Nie zostań agentem jednorazowym!"). Przekaz: rosyjskie służby werbują przez media społecznościowe „agentów niskiego poziomu"; wciągnięci ryzykują odpowiedzialność karną (do 10 lat więzienia), często nie wiedząc, dla kogo pracują. Zalecenie: nie wchodzić w kontakt, zgłaszać służbom.

Dlaczego ten model jest dla Moskwy tak wygodny

Zestawmy go z klasycznym nielegałem. Nielegał wymagał lat szkolenia, budowy legendy, ogromnych nakładów i jego dekonspiracja była katastrofą. Agent jednorazowy „kosztuje" jedną rozmowę na czacie i kilka tysięcy euro; jego dekonspiracja nic Moskwy nie kosztuje, bo nic go z Moskwą nie łączy poza kontem, które można skasować. Walker uchwycił tę różnicę już na przykładzie „wirtualnych nielegałów" IRA: fikcyjna tożsamość, którą KGB budowało latami, dziś powstaje kilkoma kliknięciami i równie szybko znika. Ta sama logika, jednorazowość, zaprzeczalność, skalowalność, napędza dziś werbunek wykonawców sabotażu.

Gdzie ten model jest słaby i to jest wiadomość dla obrońcy

Model jednorazowy ma jednak wbudowane słabości, które czynią go podatnym na wykrycie i to jest najważniejsza wiadomość tego rozdziału dla strony defensywnej.

Po pierwsze, **wykonawca jest amatorem.** Nie ma szkolenia, nie umie wykrywać obserwacji, popełnia elementarne błędy. Zostawia ślad telefonu, płaci kartą za paliwo, filmuje własne działanie, chwali się w sieci.

Po drugie, **wymóg dowodu tworzy dowód.** Nagranie żądane przez mocodawcę staje się materiałem obciążającym w sądzie.

Po trzecie, **komunikacja idzie przez platformę.** Telegram nie jest niewidzialny dla służb; konta, metadane, powiązania da się rozpracować, a współpraca międzynarodowa (Eurojust, Europol) domyka obraz.

Po czwarte, **łańcuch pośredników działa w obie strony.** Ma chronić mocodawcę, ale jednocześnie oznacza, że wielu wykonawców i pośredników wie o sobie nawzajem, a zatrzymanie jednego często prowadzi do kolejnych.

Dla obrońcy wniosek jest budujący: przeciwnik zamienił jakość na ilość, a ilość zostawia ślady. Amator jest groźny, bo jest nieprzewidywalny i gotów na przemoc, ale jest też znacznie łatwiejszy do wykrycia niż wyszkolony nielegał. Cała część szkoleniowa opiera się na tej obserwacji.

Rozdział 10. Nośniki i płatności ery cyfrowej

Skoro klasyczna martwa skrzynka jako narzędzie łączności w dużej mierze ustąpiła, warto zrozumieć, co przejęło jej funkcje. Bo funkcje pozostały te same, trzeba przekazać instrukcję, pieniądze, czasem przedmiot, zmieniły się tylko nośniki. Opisujemy je jako zjawisko do rozpoznania, nie jako poradnik.

Instrukcja: komunikator zamiast sygnału

Funkcję przekazu instrukcji przejął szyfrowany komunikator. To, co dawniej wymagało systemu sygnałów i skrzynki, dziś załatwia czat: zadanie, adres, termin, forma dowodu. Zaletą dla przeciwnika jest natychmiastowość i skala; wadą, że komunikacja, choć szyfrowana w treści, zostawia metadane, powiązania i urządzenia, które służby potrafią rozpracować.

Pieniądze: kryptowaluta zamiast gotówki w skrzynce

Funkcję przekazu pieniędzy w dużej mierze przejęły kryptowaluty, wypłacane „po wykonaniu". W sprawach europejskich wielokrotnie pojawia się ten sam schemat: obietnica kilku–kilkunastu tysięcy (euro, dolarów, czasem z dodatkiem w rodzaju „i BMW", jak w litewskiej sprawie podpalenia IKEA), płatna w krypto po dostarczeniu dowodu. Czeski przypadek białoruskiej dziennikarki współpracującej z GRU pokazuje, że honoraria „za usługi" liczone w dziesiątkach tysięcy euro również płynęły w kryptowalutach. Warto jednak odnotować, że gotówka nie zniknęła całkowicie, sprawa Dulcewów (setki tysięcy euro w gotówce, w tym w skrytce w lodówce) dowodzi, że przy poważniejszych, długoterminowych operacjach fizyczny pieniądz nadal krąży.

Przedmiot: łańcuch kurierski jako nośnik

Najbardziej niepokojącą innowacją jest wykorzystanie komercyjnego łańcucha kurierskiego jako nośnika i to zarówno do rozpoznania, jak i do ataku. Zamiast skrzynki w murze, przesyłka w systemie DHL czy DPD. W wariancie rozpoznawczym paczki z nadajnikami GPS śledzą trasy logistyczne (sprawa osądzona w Niemczech w 2026 roku). W wariancie ofensywnym paczki zawierają ładunki zapalające (kampania z 2024 roku, o której w rozdziale 12). To odwrócenie logiki skrzynki: dawniej chodziło o to, by przedmiot pozostał niezauważony w bezruchu; dziś przedmiot ma się poruszać w globalnym systemie, ukryty w masie milionów legalnych przesyłek.

> **SYGNAŁ OSTRZEGAWCZY: łańcuch kurierski.** Po kampanii paczek zapalających 2024 r. nietypowa przesyłka nie jest już wyłącznie problemem służby pocztowej. Dla obiektu chronionego oznacza to konieczność procedur przyjmowania przesyłek: nieoczekiwane paczki, nadawcy niepasujący do profilu, przesyłki „testowe" bez wartości handlowej, anomalie wagi/zapachu/temperatury. Rozdział

> 24 i moduł ochrony obiektu rozwijają procedurę.

Rozpoznanie: dron i telefon zamiast fotografa

Wreszcie funkcję rozpoznania przejęły dron i telefon komórkowy. Rozpoznanie obiektów, kiedyś zadanie wymagające agenta na miejscu, dziś realizuje amator z telefonem albo tani dron. Fala naruszeń przestrzeni powietrznej nad obiektami wrażliwymi w Europie w latach 2025–2026 (drony nad lotniskami, bazami, portami; incydent z dronem z ładunkiem przy samolocie cargo w Lipsku w sierpniu 2026 roku) pokazuje, że rozpoznanie i sabotaż zlewają się w jedno, a nośnikiem bywa urządzenie kupione w sklepie.

Wniosek: nośniki nowe, logika stara

Zwróćmy uwagę na ciągłość. Wszystkie cztery funkcje, instrukcja, pieniądze, przedmiot, rozpoznanie, to dokładnie te same funkcje, które realizowała klasyczna łączność bezosobowa. Zmienił się nośnik, nie logika. I dobra wiadomość dla obrońcy jest taka sama jak w rozdziale 9: każdy z nowych nośników zostawia ślad, którego skrzynka w murze nie zostawiała. Komunikator ma metadane. Krypto ma łańcuch transakcji. Paczka ma nadawcę, wagę i trasę. Dron ma sygnaturę i operatora. Przeciwnik zyskał skalę i szybkość, ale zapłacił za nie śladem.

Rozdział 11. Mapa kampanii 2022–2026 kraj po kraju

Ten rozdział jest przeglądowy: pokazuje skalę i geografię rosyjskiej kampanii hybrydowej w Europie od inwazji do połowy 2026 roku. Dla polskiej firmy ochrony czy działu bezpieczeństwa jest to mapa środowiska, w którym działa. Poszczególne sprawy z bliska opisuje rozdział 12.

Polska, kraj frontowy hybrydowo

Polska, jako główny lądowy korytarz wsparcia dla Ukrainy, jest jednym z najintensywniej atakowanych państw. Agencja Bezpieczeństwa Wewnętrznego, po czternastoletniej przerwie wznowiła publikację jawnych raportów rocznych, ujawniając skalę wcześniej nieujawnianą: ponad 60 śledztw szpiegowskich w latach 2024–2025 i 82 osoby, którym postawiono zarzuty od czasu pełnoskalowej inwazji. To najwyższe liczby od lat dziewięćdziesiątych. Rzecznik ministra koordynatora służb specjalnych informował o 55 osobach zatrzymanych w związku z sabotażem i szpiegostwem „w ciągu ostatnich mniej więcej trzech lat".

ABW opisała dwa niepokojące trendy. Po pierwsze, **profesjonalizację**: odejście od amatorskich pojedynczych agentów ku zorganizowanym strukturom, rosnące wykorzystanie internetu i kryptowalut do werbunku i płatności. Po drugie, **gotowość do ofiar cywilnych**: rozpoznanie obejmowało obiekty cywilne (centra handlowe, obiekty użyteczności publicznej), a przeciwnik godził się na ofiary wśród ludności. Kulminacją był sabotaż linii kolejowej Warszawa–Lublin–Hrubieszów w listopadzie 2025 roku (rozdział 12), który premier określił jako „być może najpoważniejszą sytuację dla bezpieczeństwa narodowego od wybuchu pełnoskalowej wojny".

> **RAMKA FAKTOGRAFICZNA: Polska w liczbach (raport ABW, 2024–2025).** Ponad 60 śledztw o szpiegostwo; 82 osoby z zarzutami od lutego 2022; ok. 55 osób zatrzymanych w ciągu ~3 lat. Główne zagrożenie: rosyjskie i białoruskie służby, w mniejszym stopniu chińskie. Trend: profesjonalizacja, werbunek przez internet i płatności w krypto, rozpoznanie obiektów cywilnych i wojskowych, gotowość do ofiar cywilnych.

Litwa, węzeł paczek zapalających i celownik na dysydentów

Litwa okazała się węzłem kampanii przesyłek zapalających z 2024 roku: to z Wilna nadano paczki z ładunkami, które zapaliły się w Niemczech, Polsce i Wielkiej Brytanii (proces pięciu oskarżonych ruszył w Wilnie w kwietniu 2026 roku; śledztwo wskazało 22 osoby). Litwa była też celem siatki planującej zabójstwa na zlecenie, rozbitej w 2025–2026 roku dzięki współpracy z Ukrainą, obejmującej obywateli siedmiu państw.

Niemcy, od podpaleń po drony nad cargo

Niemcy, główny europejski dostawca uzbrojenia dla Ukrainy, zmierzyły się z całym spektrum: paczka zapalająca w węźle DHL w Lipsku (lipiec 2024), zatrzymania obywateli niemiecko-rosyjskich planujących zamachy na obiekty wojskowe i przemysłowe (2024), sprawa paczek z GPS śledzących logistykę (wyrok w Stuttgarcie w sierpniu 2026), wreszcie dron z ładunkiem wykryty przy samolocie cargo na lotnisku Lipsk-Halle w sierpniu 2026 roku, opisany przez ministra spraw wewnętrznych jako możliwy „scenariusz ataku hybrydowego". To Niemcy uruchomiły kampanię „Kein Wegwerf-Agent".

Wielka Brytania, pierwsze wyroki z nowej ustawy

Wielka Brytania stała się miejscem pierwszych skazań na podstawie nowej ustawy o bezpieczeństwie narodowym (National Security Act 2023). Podpalenie magazynu z pomocą i sprzętem Starlink dla Ukrainy w londyńskim Leyton (marzec 2024), zlecone przez Grupę Wagnera, zakończyło się w październiku 2025 roku wyrokami do 17 lat więzienia (rozdział 12). We wrześniu 2025 roku Wielka Brytania zatrzymała trójkę podejrzanych o sabotaż na rzecz Rosji.

Czechy, rozpoznanie werbunku migrantów

Czeska BIS opisała rosyjski werbunek migrantów spoza UE przez Telegram do rozpoznania i sabotażu, a w 2025 roku ujawniła sprawę białoruskiej dziennikarki (Natalia Sudliankowa) współpracującej z GRU i opłacanej w kryptowalutach; po sprawie wydalono rosyjskich dyplomatów i objęto zamieszanych sankcjami.

Estonia, Łotwa, Norwegia, Włochy i inni

Estonia odnotowała serię aktów wandalizmu, dewastacji pomników i samochodów urzędników, w tym z udziałem nieletnich; zapadły wyroki. Łotwa skazała za szpiegostwo młodych ludzi zwerbowanych do rozpoznania bazy NATO i podpaleń. Norwegia aresztowała nielegała GRU podającego się za brazylijskiego naukowca (José Assis Giammaria), pracującego, jak na ironię, w instytucie oceniającym zagrożenia hybrydowe. Włochy w 2026 roku zatrzymały dwie osoby (w tym byłego funkcjonariusza) pod zarzutem szpiegostwa na rzecz Rosji. Do tego dochodzi seria uszkodzeń podmorskich kabli na Bałtyku, przypisywana „flocie cieni", która wywołała natowską operację Baltic Sentry, oraz fala naruszeń przestrzeni powietrznej przez drony, na którą NATO odpowiedziało operacją Eastern Sentry (2025).

Odczyt mapy dla polskiej firmy

Z tej mapy płyną trzy praktyczne wnioski dla polskiego działu bezpieczeństwa. Po pierwsze, **Polska jest w pierwszej linii**, nie jest to zagrożenie „gdzieś w Europie", lecz zjawisko lokalne, potwierdzone raportami ABW i wyrokami. Po drugie, **cele są rozproszone i cywilne**, kolej, logistyka, magazyny, energetyka, ale też centra handlowe; „niewojskowy" charakter obiektu nie wyłącza go z kręgu celów. Po trzecie, **wykonawcy są miejscowi i amatorscy**, co przesuwa ciężar obrony z klasycznego kontrwywiadu na codzienną czujność ochrony fizycznej, procedury przyjmowania przesyłek i świadomość personelu. To uzasadnia całą Część III.

Rozdział 11a. Profile krajowe, rozszerzenie

Rozdział 11 dał mapę. Ten rozdział pogłębia profile kilku krajów najważniejszych dla polskiego czytelnika, bo pokazuje, że kampania nie jest jednolita, w każdym kraju przybiera nieco inny kształt, zależny od jego roli we wsparciu dla Ukrainy i od zdolności jego służb.

Polska, laboratorium zagrożenia i odpowiedzi

Polska łączy dwie cechy, które czynią ją modelowym przypadkiem: jest głównym lądowym korytarzem wsparcia dla Ukrainy i graniczy z Białorusią, z której terytorium działa część siatek. Skutkiem jest największa w regionie intensywność incydentów i największa liczba postępowań. Wznowienie przez ABW jawnych raportów rocznych, po czternastoletniej przerwie, jest samo w sobie odpowiedzią: jawność jako narzędzie budowania odporności społecznej.

Wzorzec polskich spraw jest pouczający. Wykonawcy to często obywatele Ukrainy lub Białorusi oraz Polacy w trudnej sytuacji, werbowani przez komunikatory. Zadania obejmują pełne spektrum: rozpoznanie obiektów wojskowych i cywilnych, przygotowywanie i wykonywanie podpaleń, rozprowadzanie ładunków, wreszcie sabotaż kolejowy. Sprawa Mika/Puławy pokazała, że przeciwnik jest gotów do ataków mogących zagrozić życiu (pociąg z 473 pasażerami) i że wykonawcy zbiegają następnie na Białoruś, korzystając z bliskości granicy. Odpowiedzią stały się operacje ochrony infrastruktury i mobilizacja tysięcy żołnierzy do dozoru newralgicznych odcinków.

Dla polskiej firmy ochrony wniosek jest bezpośredni: to nie jest zagrożenie „europejskie” w sensie odległym, lecz codzienne środowisko pracy. Obiekty związane z logistyką, koleją, energetyką, obronnością i wsparciem dla Ukrainy są w kręgu zainteresowania i to one najbardziej potrzebują warstwy czujników opisanej w Części III.

Niemcy, połączenie ścigania i uświadamiania

Niemcy, jako główny europejski dostawca uzbrojenia dla Ukrainy, są celem szczególnie różnorodnym: od podpaleń, przez paczki (zapalające i z GPS), po drony nad obiektami wojskowymi i cargo. Niemiecka odpowiedź wyróżnia się połączeniem twardego ścigania (procesy o szpiegostwo w celu sabotażu, zagrożenie karą do dziesięciu lat) z bezprecedensową otwartością informacyjną: wspólna kampania czterech służb „Kein Wegwerf-Agent werden!” jest wzorem publicznego ostrzegania. Niemiecki przypadek pokazuje, że represja i prewencja przez świadomość nie wykluczają się, lecz wzmacniają.

Wielka Brytania, nowe prawo w działaniu

Brytania wniosła do europejskiej odpowiedzi nowe narzędzie prawne, National Security Act 2023 i natychmiast je zastosowała w sprawie Leyton. Znaczenie tej sprawy wykracza poza jeden wyrok:

pokazała, że lokalnego pośrednika działającego przez Telegram można skazać jako sprawcę przestępstwa na rzecz obcego państwa, z wieloletnim wyrokiem. To precedens odstraszający, który zmienia kalkulację potencjalnego rekruta: „drobna fucha” okazuje się zbrodnią na rzecz obcego mocarstwa.

Kraje bałtyckie, pierwsza linia i pełne spektrum

Litwa, Łotwa i Estonia, jako państwa frontowe i bezpośredni sąsiedzi Rosji, doświadczają pełnego spektrum: od wandalizmu i dewastacji pomników (Estonia, z udziałem nieletnich), przez rozpoznanie baz NATO i podpalenia (Łotwa), po węzeł paczek zapalających i cel siatki zabójstw (Litwa). Kraje te, o niewielkich zasobach, kompensują je wysoką czujnością społeczną, sprawnym kontrwywiadem i ścisłą współpracą regionalną. Estoński przypadek udziału nieletnich w aktach sabotażu jest ostrzeżeniem o rozszerzaniu puli rekrutów na osoby bardzo młode, radykalizowane w sieci.

Kierunek morski, Bałtyk i infrastruktura podmorska

Osobnym teatrem jest Bałtyk, gdzie seria uszkodzeń kabli telekomunikacyjnych i energetycznych, przypisywana „flocie cieni” (statkom o niejasnej własności, ciągnącym kotwice po dnie), pokazała podatność infrastruktury podmorskiej. NATO odpowiedziało operacją Baltic Sentry, wzmożoną obecnością i szybszą atrybucją. Problem morski ilustruje szerszą prawdę o infrastrukturze rozproszonej: nie da się fizycznie ochronić każdego metra, więc obrona opiera się na czujnikach, szybkiej reakcji, redundancji i odstraszaniu przez wykrywalność.

Wniosek z profili

Mimo różnic kraj po kraju powtarza się ten sam schemat: cele związane ze wsparciem dla Ukrainy, wykonawcy lokalni i amatorscy werbowani zdalnie, zaprzeczalność mocodawcy, a po stronie obrony, rosnąca rola jawności, świadomości społecznej i współpracy międzynarodowej. Różni się natężenie i akcent, nie mechanizm. To potwierdza uniwersalność metod obrony opisanych w tym opracowaniu.

Rozdział 12. Sześć spraw z bliska

Sześć spraw, każda udokumentowana publicznie, stanowi materiał źródłowy do ćwiczeń sztabowych w rozdziale 18. Opisujemy je faktograficznie, z naciskiem na to, jak przebiegały i jak zostały wykryte.

12.1. Leyton, Londyn, podpalenie zlecone przez Wagnera (marzec 2024)

20 marca 2024 roku grupa mężczyzn podpaliła magazyn na terenie przemysłowym w londyńskim Leyton, w którym znajdowała się pomoc humanitarna i sprzęt Starlink przeznaczony dla Ukrainy. Straty sięgnęły około miliona funtów. Organizatorem był 20-letni Dylan Earl, który przez Telegram zgłosił Grupie Wagnera gotowość do „misji" i zrekrutował wykonawców. Zebrany materiał, nagranie z podpalenia transmitowane przez jednego ze sprawców do Earla, zapisy CCTV i kamer drogowych, dane telefonów, DNA na nożu, zapisy zakupu paliwa, wiadomości z komunikatora Signal, pozwolił skazać sześciu mężczyzn. Earl i Jake Reeves jako pierwsi w historii zostali skazani z National Security Act 2023. Wyroki (październik 2025): od 7 do 17 lat więzienia.

> **RAMKA FAKTOGRAFICZNA: Leyton.** Cel: magazyn pomocy i sprzęt Starlink dla Ukrainy. Zleceniodawca: Grupa Wagnera przez Telegram. Wykonawcy: lokalni, młodzi, zwerbowani przez pośrednika. Dowody obciążające w dużej mierze wytworzone przez samych sprawców (transmisja nagrania, ślady cyfrowe, zakupy). Wyroki 7–17 lat, pierwsze skazania z NSA 2023.

12.2. Paczki zapalające DHL/DPD (lipiec 2024)

W lipcu 2024 roku z Wilna nadano cztery przesyłki z domowej roboty ładunkami zapalająco-wybuchowymi, ukrytymi m.in. w urządzeniach do masażu z substancją na bazie magnezu. Ładunki zapaliły się w węzłach w Niemczech (Lipsk), Polsce i Wielkiej Brytanii (Birmingham). Dwie przesyłki testowe dotarły do USA i Kanady; dwie kolejne przechwycono w Amsterdamie. Polscy śledczy ocenili incydent w Birmingham jako „próbę generalną" przed uderzeniem w logistykę transatlantycką, gdyby ładunek zapalił się na pokładzie samolotu, skutki byłyby katastrofalne. Powołano wspólny zespół śledczy przy Eurojust (Litwa, Polska, Niemcy, Holandia, Wielka Brytania, przy wsparciu Estonii, Łotwy, USA, Kanady, Europolu). Śledztwo wskazało 22 osoby wspierające rosyjski wywiad; proces pięciu oskarżonych ruszył w Wilnie w kwietniu 2026 roku. Rekrutów, z Litwy, Polski, Rosji, Ukrainy i Łotwy, pozyskano przez komunikatory, z podziałem zadań między pośredników.

12.3. Sabotaż kolejowy pod Mika i Puławami (listopad 2025)

W nocy z 16 na 17 listopada 2025 roku doszło do dwóch aktów sabotażu na strategicznej linii Warszawa–Lublin–Hrubieszów, którą płynie wsparcie dla Ukrainy. Pod miejscowością Mika (ok. 100 km na południowy wschód od Warszawy) ładunek, według ustaleń materiał typu C-4, zdetonowano przy przejeździe pociągu

towarowego, uszkadzając tory i sieć trakcyjną. Dzień później, w rejonie Puław, w tor wklinowano metalowy element i zerwano przewody trakcyjne przy pociągu z 473 pasażerami. Polskie służby przypisały czyny dwóm obywatelom Ukrainy (Ołeksandr K. i Jewhenij I.) działającym na rzecz FSB; jeden miał wcześniejszą karalność za sabotaż we Lwowie, drugi pochodził z okupowanego Doniecka. Sprawcy zbiegli do Białorusi. 2 grudnia polska prokuratura postawiła zarzuty obywatelowi Rosji jako organizatorowi siatki „szpiegowsko-sabotażowej" powiązanej z FSB. Uruchomiono operacje ochrony infrastruktury (m.in. z udziałem tysięcy żołnierzy). Sprawa trafiła nawet do amerykańskiej dorocznej oceny zagrożeń jako przykład sabotażu infrastruktury krytycznej w Europie.

> **RAMKA FAKTOGRAFICZNA: Mika/Puławy.** Data: 16–17 listopada 2025. Cel: linia kolejowa wsparcia dla Ukrainy. Metoda: ładunek (C-4) i sabotaż mechaniczny toru. Sprawcy: obywatele Ukrainy na rzecz FSB, zbiegli do Białorusi. Reakcja: zarzuty dla rosyjskiego organizatora, operacje ochrony infrastruktury, najwyższy poziom alarmu politycznego.

12.4. Siatka zabójstw i sabotażu rozbita z udziałem Ukrainy (2025–2026)

W kwietniu 2026 roku organy ścigania Ukrainy i państw partnerskich ujawniły rozbicie siatki, która od sierpnia 2024 roku planowała zabójstwa na zlecenie i sabotaż w UE. Głównym celem była Litwa, inwigilowano m.in. rosyjskiego dysydenta z azylem politycznym. W siatce działali obywatele Ukrainy, Rosji, Białorusi, Gruzji, Łotwy, Mołdawii i Grecji. Litwa postawiła zarzuty 13 osobom (9 zatrzymanych, 4 objęte europejskim nakazem aresztowania). Sprawa pokazuje pełne spektrum: od rozpoznania obiektów wojskowych, przez sabotaż, po planowane zabójstwa.

12.5. Paczki z GPS śledzące logistykę (wyrok 2026)

W sierpniu 2026 roku sąd w Stuttgarcie skazał 30-letniego obywatela Ukrainy za „szpiegostwo w celu sabotażu": nadawał przesyłki testowe z nadajnikami GPS w kierunku Ukrainy, by rozpoznać i zakłócić trasy transportu i infrastrukturę logistyczną. Dwaj współoskarżeni zostali uniewinnieni z braku dowodów. Sprawa ilustruje wariant rozpoznawczy wykorzystania łańcucha kurierskiego, paczka jako sensor, nie jako broń.

12.6. Dulcewowie, koniec klasycznego nielegała (2022–2024)

Sprawę Anny i Artioma Dulcewów opisaliśmy w rozdziale 7. Wracamy do niej tu jako do materiału ćwiczeniowego, bo domyka spektrum: od amatorskiego wykonawcy jednorazowego (Leyton, paczki) po wyszkolonego nielegała żyjącego dekadę pod obcą tożsamością. Zestawienie tych skrajności w jednym rozdziale nie jest przypadkowe, pokazuje, że przeciwnik operuje jednocześnie na obu krańcach: taniego, masowego proxy i drogiego, głębokiego nielegała. Obrona musi umieć rozpoznawać oba.

Rozdział 13. Dlaczego siatki proxy wpadają

Zamykając Część II, zbierzmy, analogicznie do rozdziału 5, powtarzalne przyczyny, dla których współczesne siatki proxy są wykrywane. Ten katalog jest pomostem do części szkoleniowej: każda przyczyna wpadki to jednocześnie punkt, w którym obrońca może zadziałać.

Amatorstwo wykonawcy. Rekrut bez szkolenia nie umie wykrywać obserwacji, nie zna zasad bezpieczeństwa, działa impulsywnie. Zostawia telefon włączony, płaci kartą, chwali się w sieci, wraca w to samo miejsce. To najczęstsza przyczyna wpadek w modelu jednorazowym.

Dowód wytworzony na żądanie. Wymóg nagrania działania, konieczny, by wykonawca dostał zapłatę, tworzy gotowy materiał dowodowy. W sprawie Leyton to transmisja z podpalenia domknęła sprawę.

Ślad cyfrowy i płatniczy. Metadane komunikatora, łańcuch transakcji krypto, dane lokalizacyjne, CCTV, kamery drogowe, rejestry przesyłek. Amator nie potrafi tego wszystkiego wyczyścić; każdy z tych śladów da się zestawić z pozostałymi.

Łańcuch pośredników działa w obie strony. Kompartmentalizacja chroni mocodawcę, ale sieć pośredników i wykonawców jest gęsta; zatrzymanie jednego ogniwa prowadzi do kolejnych. Sprawy litewska i paczkowa to sieci kilkunastu–dwudziestu kilku osób.

Współpraca międzynarodowa. Wspólne zespoły śledcze (Eurojust), Europol, wymiana danych między służbami sprawiają, że operacja rozpięta na kilka krajów jest ścigana łącznie, a nie w izolowanych fragmentach.

Biały wywiad (OSINT). Grozev i Bellingcat pokazali, że rozpoznawanie twarzy, wycieki baz danych i cyfrowe ślady (nawet mikroczip kota) potrafią zdemaskować nawet wyszkolonego nielegała. Wobec amatora OSINT działa jeszcze skuteczniej.

Czujność obywatela i personelu. Wiele spraw zaczęło się od zgłoszenia, zaniepokojonego świadka, pracownika, sąsiada. To jest ten punkt, na który obrona ma największy wpływ i któremu poświęcona jest Część III. Kampanie takie jak „Kein Wegwerf-Agent”, apele SUPO, BIS czy ABW mają dokładnie ten cel: zamienić milionów obywateli w czujników.

Podsumowanie Części II

Inwazja lutego 2022 zamknęła Moskwie dwie tradycyjne drogi operacji w Europie, dyplomatów pod przykryciem i „turystów” z rosyjskim paszportem i wypchnęła rosyjski wywiad ku dwóm rozwiązaniom: powrotowi klasycznych nielegałów z tożsamością państw trzecich oraz, na masową skalę, ku siatkom jednorazowych wykonawców werbowanych przez Telegram i opłacanych w kryptowalutach. Funkcje dawnej łączności bezosobowej, instrukcja, pieniądze, przedmiot, rozpoznanie, przejęły nośniki cyfrowe i łańcuch kurierski. Cel przesunął się z kradzieży tajemnic ku sabotażowi i zastraszaniu, a geografia, ku logistyce wsparcia dla Ukrainy, z Polską w pierwszej linii. Przeciwnik zyskał skalę, szybkość i zaprzeczalność, ale

zapłacił za to śladem i amatorstwem wykonawców. To właśnie ten ślad i to amatorstwo czynią obronę możliwą i to jest przedmiot Części III.

CZĘŚĆ III. MODUŁ SZKOLENIOWY (DEFENSYWNY)

Rozdział 14. Cele, odbiorcy i zasady modułu

Po co ten moduł istnieje

Części I i II pokazały, jak działa przeciwnik. Część III uczy, jak go rozpoznać i jak zareagować, zgodnie z prawem i w granicach roli osoby szkolonej. To jest moduł czysto defensywny (white-hat). Nie uczy prowadzenia operacji; uczy je wykrywać i udaremniać.

Cel nadrzędny modułu można ująć jednym zdaniem: **zamienić personel organizacji w warstwę czujników, która wychwytuje anomalię, zanim przerodzi się ona w szkodę i przekazuje ją właściwym ludziom we właściwy sposób.** Cała reszta, fazy, wskaźniki, karty pracy, ćwiczenia, służy temu jednemu celowi.

Kto jest odbiorcą

Moduł jest skalowalny i przewiduje trzy poziomy odbiorców.

Poziom 1, cały personel (świadomość). Każdy pracownik, także niezwiązany z bezpieczeństwem: recepcja, magazyn, kierowcy, administracja, personel miejscowy placówki. Ich zadaniem nie jest prowadzenie śledztw, lecz rozpoznanie sygnału i jego zgłoszenie. Dla nich przeznaczone są rozdziały 15, 16 (w części podstawowej), 19 i test z rozdziału 20.

Poziom 2, ochrona fizyczna i oficerowie bezpieczeństwa. Personel ochrony, patrole, kierownicy zmian, oficerowie bezpieczeństwa obiektu. Dla nich, całość Części III, w tym karty pracy (17), moduły surveillance detection i ochrony obiektu, oraz ćwiczenia (18).

Poziom 3, kadra kierownicza i analitycy bezpieczeństwa. Osoby decydujące o polityce bezpieczeństwa, kontaktach ze służbami, procedurach. Dla nich, całość, ze szczególnym uwzględnieniem Części IV.

Cztery zasady, które obowiązują przez cały moduł

Zasada anomalii na tle normy. Nie szukamy „szpiega”. Szukamy odstępstwa od normalnego rytmu, który znamy. Warunkiem wstępnym jest więc znajomość normy własnego obiektu. Kto nie zna normy, nie rozpozna anomalii.

Zasada wielu wskaźników. Pojedynczy sygnał niczego nie dowodzi i nie wolno na jego podstawie nikogo oskarżać. Dopiero zbieg kilku niezależnych wskaźników w czasie uzasadnia zgłoszenie. Uczymy sumowania, nie pochopnych wniosków.

Zasada roli. Osoba szkolona działa w granicach swojej roli. Ochroniarz zabezpiecza i zgłasza, nie prowadzi przesłuchań, nie zatrzymuje na własną rękę, nie „rozpracowuje” podejrzanego. Przekroczenie roli niszczy dowody, naraża osobę i bywa nielegalne.

Zasada zgłoszenia bez etykietowania. Zgłaszamy fakty i obserwacje, nie oceny i etykiety. „Widziałem osobę fotografującą bramę i ogrodzenie przez dwadzieścia minut, oto godzina i opis", a nie „złapałem rosyjskiego szpiega". Etykieta uprzedza fakty, naraża na błąd i na krzywdę osoby niewinnej.

> **UWAGA OPSEC: dwustronna.** Zasada zgłoszenia bez etykietowania chroni dwie strony naraz. Chroni organizację przed fałszywym alarmem i pomówieniem. I chroni prywatność oraz bezpieczeństwo osób postronnych, a także źródeł i osób współpracujących ze służbami, które nie powinny być publicznie nazywane ani „namierzane" przez amatorów. Kanał zgłoszenia ma być zamknięty i wąski (rozdział 19), właśnie po to, by informacja o potencjalnym zagrożeniu sama nie stała się wyciekiem.

Format prowadzenia szkolenia

Zalecany format dla poziomu 2 to jeden dzień: rano teoria (Część II w pigułce + rozdziały 15–16), po południu warsztat (karty pracy 17 + jedno ćwiczenie tabletop z 18), na koniec test (20). Dla poziomu 1 wystarczy sesja 90-minutowa: skrót zagrożenia, fazy werbunku, katalog sygnałów, procedura zgłoszenia, test. Dla poziomu 3, półdniowy warsztat decyzyjny oparty na Części IV i dwóch ćwiczeniach tabletop.

Rozdział 15. Cykl werbunkowy w sześciu fazach

Rozdział rozwija sześciofazowy model z rozdziału 9 w narzędzie szkoleniowe: dla każdej fazy podajemy, jak wygląda z zewnątrz, po czym ją poznać i co robić. Model odnosi się do dwóch scenariuszy naraz: werbunku osoby z zewnątrz oraz, co ważne dla działu bezpieczeństwa, werbunku własnego pracownika lub personelu miejscowego.

Faza 1, kontakt

Jak wygląda. Nagabywanie w komunikatorze lub mediach społecznościowych. „Łatwa praca, dobre pieniądze, napisz na Telegramie". Oferta pracy dorywczej bez jasnego pracodawcy. Może przyjść jako wiadomość od nieznajomego, komentarz, ogłoszenie w grupie, kontakt „przez znajomego".

Po czym poznać. Anonimowy lub słabo zidentyfikowany nadawca. Nieproporcjonalnie wysoka zapłata do trywialnego zadania. Nacisk na komunikator szyfrowany od pierwszej wiadomości. Pytania o sytuację finansową, karalność, poglądy, dostęp do obiektów.

Co robić. Nie odpowiadać. Nie kasować (zachować jako dowód). Zgłosić, pracownik przełożonemu i bezpieczeństwu, osoba prywatna właściwej służbie.

Faza 2, test

Jak wygląda. Drobne, „niewinne" zadanie: zrób zdjęcie budynku, rozwieś plakaty, przewieź lub nadaj paczkę, sprawdź, czy coś jest na miejscu. Zapłata mała, ale realna.

Po czym poznać. To jest faza krytyczna, moment, w którym człowiek jeszcze uważa, że „nic złego nie robi", a już zostaje wciągnięty. Wskaźnik: zadanie bez sensownego uzasadnienia biznesowego, dotyczące obiektu, infrastruktury lub przesyłki, z wymogiem dyskrecji i dowodu wykonania.

Co robić. Tu przebiega granica. Po wykonaniu „testu" człowiek jest już uwikłany i podatny na szantaż. Przekaz szkoleniowy: jeśli pierwsze zadanie dotyczy fotografowania obiektów, przewożenia paczek czy oznaczania miejsc dla nieznanego zleceniodawcy, to nie jest praca dorywcza, to faza 2. Wycofać się i zgłosić natychmiast, zanim zapłata zamieni się w haczyk.

> **SYGNAŁ OSTRZEGAWCZY: faza 2 wobec własnego personelu.** Pracownik, który nagle wykonuje drobne, nietypowe czynności poza zakresem obowiązków, fotografuje części obiektu bez powodu, wypytuje o grafiki ochrony, „przypadkiem" interesuje się przesyłkami lub dostępami, może być w fazie 2, świadomie lub nie. Reakcją nie jest oskarżenie, lecz odnotowanie i zgłoszenie zgodnie z zasadą wielu

> wskaźników.

Faza 3, eskalacja

Jak wygląda. Zadania rosną: obserwacja z notowaniem, podpalenie, wandalizm, podłożenie przedmiotu, w skrajności ładunek. Zapłata rośnie z ryzykiem.

Po czym poznać. Wyraźnie przestępczy charakter zadania; presja czasu; odwołanie do wcześniejszego „testu" jako dźwigni („już to zrobiłeś, teraz zrób to").

Co robić. Na tym etapie mowa już o poważnych przestępstwach. Zgłoszenie do służb jest nie tylko właściwe, lecz często jedyną drogą wyjścia bez wyroku. Kampanie służb (SUPO, BKA) podkreślają: zgłaszający wcześnie ma szansę uniknąć odpowiedzialności; wykonawca, nie.

Faza 4, dowód wykonania

Jak wygląda. Wymóg sfilmowania działania jako warunek zapłaty.

Po czym poznać. Żądanie nagrania czynu, czegoś, czego żaden legalny pracodawca nie wymaga.

Znaczenie dla obrony. Ten wymóg to największa słabość przeciwnika. Nagranie lokalizuje wykonawcę w czasie i miejscu i staje się dowodem. Dla śledczego to prezent; dla wykonawcy, pętla.

Faza 5, zatrzymanie

Jak wygląda. Szybka reakcja służb, zatrzymanie, zarzuty, często z katalogu działań na rzecz obcego państwa lub o charakterze terrorystycznym.

Realia. Wyroki są wysokie (Leyton: do 17 lat; niemieckie ostrzeżenia: do 10 lat; polskie sprawy sabotażu: zagrożenie karą wieloletniego więzienia). To nie jest „drobna fucha".

Faza 6, konsekwencje

Jak wygląda. Mocodawca znika. Wsparcia brak. Wykonawca zostaje sam z wyrokiem w obcym kraju.

Przekaz. To jest istota terminu „agent jednorazowy". Cała wartość rekruta dla Moskwy polega na tym, że jest wymienny i że jego utrata nic nie kosztuje. Ktokolwiek daje się wciągnąć, wciąga się w rolę materiału zużywalnego. To najsilniejszy argument prewencyjny i tak należy go przedstawiać w szkoleniu.

Diagram cyklu (do slajdu)

Kontakt, Test, Eskalacja, Dowód, Zatrzymanie, Konsekwencje. Strzałka obrony wchodzi najskuteczniej między fazą 1 a 2 (zanim padnie pierwsze „niewinne" zadanie) i musi wejść najpóźniej przy fazie 2/3. Im później, tym mniejsze pole na wyjście bez odpowiedzialności.

Rozdział 16. Katalog sygnałów ostrzegawczych

Rozdział zbiera wskaźniki w cztery grupy. Zbiorczą kartę do wydruku zawiera Dodatek C. Powtarzamy zasadę: pojedynczy wskaźnik to nie dowód; liczy się zbieg kilku i odstępstwo od normy.

Grupa A, sygnały werbunku (personel i osoby z zewnątrz)

- Niezamówione oferty pieniędzy za „drobne zadania” przez media społecznościowe lub komunikator.
- Zadania dotyczące fotografowania obiektów, przewożenia lub nadawania przesyłek, oznaczania miejsc, bez sensownego uzasadnienia.
- Nacisk na szyfrowany komunikator i dyskrecję od początku.
- Wymóg filmowania czynności.
- Pośrednik zamiast jawnego pracodawcy; płatność w kryptowalucie.
- U pracownika: nagłe, niewyjaśnione zainteresowanie grafikami ochrony, dostępami, przesyłkami, rozmieszczeniem kamer; nagła zmiana sytuacji finansowej; podatność na szantaż (długi, uzależnienia, tajemnice).

Grupa B, sygnały rozpoznania obiektu (hostile reconnaissance)

- Osoby fotografujące lub filmujące bramy, ogrodzenia, kamery, posterunki, punkty dostępu, zwłaszcza powtarzalnie i z nietypowych pozycji.
- Pytania (osobiście, telefonicznie, mailowo) o procedury ochrony, grafiki, obsadę, drogi dostaw, godziny.
- Pojazdy lub osoby pojawiające się powtarzalnie bez wyjaśnienia; „testowanie” reakcji ochrony (np. wejście i wycofanie się).
- Drony nad obiektem lub w jego pobliżu.
- Pozostawione lub „zgubione” przedmioty w pobliżu punktów wrażliwych; nietypowe, powtarzalne oznaczenia.

Grupa C, sygnały łączności bezosobowej i podłożenia

- Przedmiot pozostawiony w miejscu, gdzie nikt nic nie zostawia; przedmiot „zbyt czysty/nowy” jak na otoczenie.
- Powtarzalny, z pozoru bezsensowny znak lub przedmiot pojawiający się i znikający w rytmie skorelowanym z czyimś zachowaniem.
- Osoba zatrzymująca się na moment w punkcie bez powodu, wykonująca krótką czynność przy elemencie otoczenia i odchodząca.

- Nieoczekiwane przesyłki niepasujące do profilu obiektu; nadawcy anonimowi; paczki „testowe” bez wartości handlowej; anomalie wagi, zapachu, wycieku, temperatury, dźwięku.

Grupa D, sygnały głębokiego przykrycia (nielegał)

- Konsekwentne unikanie fotografii.
- „Firma” o ubogiej, pretekstowej działalności, służąca głównie jako uzasadnienie podróży lub obecności.
- Duże ilości gotówki bez pokrycia w widocznej działalności.
- Podejrzanie gładka, mało konkretna biografia z odległego kraju, trudna do lokalnej weryfikacji; „zabawny akcent” niepasujący do deklarowanego pochodzenia.
- Kontakty towarzyskie ukierunkowane na osoby z dostępem (wojsko, administracja, obronność) nieproporcjonalnie do deklarowanego zawodu.

> **UWAGA: ryzyko fałszywego alarmu i uprzedzeń.** Wiele z tych zachowań ma całkowicie niewinne wyjaśnienia. Turysta fotografuje architekturę. Cudzoziemiec ma akcent. Ktoś płaci gotówką. Dlatego obowiązuje zasada wielu wskaźników i zasada zgłoszenia bez etykietowania. Szkolenie musi wprost przestrzegać przed profilowaniem po narodowości, wyglądzie czy języku, to nie tylko krzywdzące i często nielegalne, ale i nieskuteczne: prowadzi do szumu, w którym ginie realny sygnał.

Rozdział 17. Karty pracy i listy kontrolne

Rozdział zawiera gotowe do wydruku karty do użytku operacyjnego i szkoleniowego. Można je kopiować i wdrażać jako załączniki do procedur bezpieczeństwa organizacji, dostosowując do prawa i regulacji wewnętrznych.

Karta 1, Obserwacja podejrzanego zachowania (dla ochrony)

Wypełnij faktami, nie ocenami. Nie konfrontuj, nie zatrzymuj na własną rękę.

- Data i godzina rozpoczęcia / zakończenia obserwacji: ____
- Miejsce (dokładny punkt obiektu): ____
- Co dokładnie zaobserwowano (czynność, nie interpretacja): ____
- Osoba: przybliżony wygląd, ubiór, cechy widoczne (bez domysłów o narodowości/pochodzeniu): ____
- Pojazd (jeśli): typ, kolor, nr rej. jeśli bezpiecznie widoczny: ____
- Czy zachowanie się powtarza? Poprzednie wystąpienia (data/godz.): ____
- Czy wykonano zdjęcia otoczenia obiektu przez osobę? Czego dotyczyły: ____
- Czy osoba pytała o procedury/grafiki/dostęp? Treść pytań: ____
- Świadkowie: ____
- Zabezpieczony materiał (zapis CCTV, godzina/kamera): ____
- Komu i o której zgłoszono: ____
- Podpis / identyfikator zgłaszającego: ____

Karta 2, Podejrzany przedmiot / przesyłka (dla ochrony i personelu)

Zasada nadrzędna: NIE dotykaj, NIE otwieraj, NIE przemieszczaj, NIE zanurzaj w wodzie, NIE używaj telefonu/radia tuż przy przedmiocie, jeśli procedura obiektu tak stanowi. Zabezpiecz strefę i wezwij właściwe służby.

- Lokalizacja przedmiotu (dokładnie): ____
- Kto i kiedy zauważył: ____
- Opis przedmiotu (rozmiar, kształt, oznaczenia, nadawca jeśli przesyłka): ____
- Dlaczego wzbudził podejrzenie (anomalia: miejsce/waga/zapach/wyciek/dźwięk/przewody/nadawca): ____
- Czy ktokolwiek dotykał/przemieszczał: ____
- Wyznaczona strefa bezpieczeństwa i ewakuacji (zgodnie z procedurą obiektu): ____
- Powiadomione służby (godzina, kto): ____
- Osoba kierująca reakcją na miejscu: ____

Karta 3, Zgłoszenie próby werbunku (dla personelu)

- Kanał kontaktu (aplikacja, platforma, telefon, osobiście): ____
- Data i godzina pierwszego kontaktu: ____
- Dane nadawcy widoczne dla Ciebie (nick, numer, profil), NIE kontaktuj się ponownie: ____
- Treść oferty / zadania (zachowaj oryginał, zrób zrzut ekranu): ____
- Oferowana zapłata i forma (gotówka/krypto): ____
- Czy padły pytania o Twój dostęp, obowiązki, obiekt, finanse, poglądy: ____
- Co dotąd zrobiłeś w reakcji (najlepiej: nic poza zachowaniem dowodu): ____
- Komu zgłoszono w organizacji i/lub której służbie: ____

Lista kontrolna A, Przyjmowanie przesyłek w obiekcie chronionym

☐ Czy istnieje wyznaczony, odseparowany punkt przyjęć?
☐ Czy personel przyjęć zna profil normalnych nadawców i przesyłek?
☐ Czy nieoczekiwane przesyłki są weryfikowane u adresata przed otwarciem?
☐ Czy istnieje procedura dla przesyłki bez nadawcy / „testowej” / z anomalią?
☐ Czy personel wie, że po kampanii paczek zapalających 2024 to realne zagrożenie?
☐ Czy jest jasna ścieżka eskalacji i numer do wezwania służb?

Lista kontrolna B, Higiena dostępu i informacji o obiekcie

☐ Czy grafiki ochrony, obsada i procedury są chronione (need-to-know)?
☐ Czy publicznie dostępne informacje o obiekcie (strony, media społ., wizytówki, zdjęcia) są przeglądane pod kątem tego, co ujawniają przeciwnikowi?
☐ Czy personel miejscowy/podwykonawcy przechodzą szkolenie świadomości?
☐ Czy istnieje rejestr i przegląd nietypowych pytań o obiekt?
☐ Czy zgłoszenia anomalii są zbierane i okresowo analizowane pod kątem powtarzalności?

Lista kontrolna C, Insider risk (model NPSA, w skrócie)

☐ Czy istnieje proces zgłaszania obaw dotyczących współpracownika, poufny i wolny od piętna?
☐ Czy zmiany zachowania (nagłe problemy finansowe, podatność na szantaż, niewyjaśnione zainteresowanie obszarami poza rolą) są objęte świadomością kadry?
☐ Czy personel wie, że celem werbunku bywa właśnie „swój”, zwłaszcza personel miejscowy w rejonach podwyższonego ryzyka?
☐ Czy reakcją na sygnał jest wsparcie i weryfikacja, a nie natychmiastowe oskarżenie?

> **UWAGA OPSEC.** Karty celowo NIE zawierają instrukcji „jak samodzielnie śledzić”, „jak podejść niezauważenie”, „jak rozbroić”. To są czynności służb i saperów, nie ochrony. Rola osoby szkolonej kończy się na: zaobserwuj, zabezpiecz, zgłoś. Przekroczenie tej granicy niszczy dowody i naraża życie.

Rozdział 18. Ćwiczenia sztabowe (tabletop) na realnych sprawach

Cztery scenariusze oparte na sprawach z rozdziału 12. Każdy ma ten sam układ: sytuacja wyjściowa, wstrzyki (nowe informacje wprowadzane przez prowadzącego), pytania do dyskusji, punkty nauczania. Ćwiczenia są defensywne, pytają „jak byś to wykrył i co byś zrobił", nie „jak byś to przeprowadził". Zalecany czas: 45–60 minut na scenariusz, grupy 4–8 osób.

Ćwiczenie 1, Magazyn (na kanwie Leyton 2024)

Sytuacja wyjściowa. Chronisz magazyn logistyczny obsługujący m.in. transporty pomocy na wschód. Nocny patrol melduje, że dwa dni z rzędu w pobliżu bramy zatrzymywał się ten sam samochód, a pasażer robił zdjęcia ogrodzenia.

Wstrzyk 1. Pracownik zgłasza, że dostał na Telegramie ofertę „łatwej pracy": ma zrobić zdjęcia bramy magazynu za 500 euro. **Wstrzyk 2.** Nocą kamera rejestruje dwie osoby przy ogrodzeniu; jedna trzyma telefon skierowany na drugą, jakby filmowała. **Wstrzyk 3.** Rano na parkingu znaleziono kanister.

Pytania. Które sygnały i z których grup (rozdz. 16) już wystąpiły? W której fazie cyklu (rozdz. 15) jest zgłaszający pracownik? Co robisz z jego zgłoszeniem? Jak zabezpieczasz kanister (Karta 2)? Kogo i kiedy zawiadamiasz? Czego NIE robisz?

Punkty nauczania. Zbieg wskaźników z grup A i B. Pracownik jest w fazie 1/2, właściwa reakcja to zachowanie dowodu i zgłoszenie, nie wykonanie zadania. Nagrywanie się nawzajem = faza 4 (dowód), słabość przeciwnika. Kanister: strefa, brak dotyku, wezwanie służb. Rola ochrony: obserwuj–zabezpiecz–zgłoś.

Ćwiczenie 2, Przesyłka (na kanwie paczek DHL 2024)

Sytuacja wyjściowa. W punkcie przyjęć biura pojawia się nieoczekiwana paczka bez jasnego nadawcy, cięższa niż wskazywałaby zawartość deklarowana jako „urządzenie do masażu".

Wstrzyk 1. Adresat twierdzi, że niczego nie zamawiał. **Wstrzyk 2.** Z paczki wydobywa się słaby zapach spalenizny, choć nikt jej nie otwierał. **Wstrzyk 3.** Ochrona przypomina sobie komunikat o kampanii paczek zapalających.

Pytania. Co robisz w pierwszej minucie? Jaka jest strefa? Kogo ewakuujesz? Kogo wzywasz? Jak dokumentujesz (Karta 2)? Jak wyglądałaby procedura, która wychwyciłaby tę paczkę wcześniej (Lista kontrolna A)?

Punkty nauczania. Anomalia wagi + brak zamówienia + zapach = trójskładnikowy sygnał grupy C. Zasada „nie dotykaj/nie otwieraj/nie zanurzaj”. Wartość procedury przyjęć. Realność zagrożenia po 2024.

Ćwiczenie 3, Kolej / infrastruktura liniowa (na kanwie Mika/Puławy 2025)

Sytuacja wyjściowa. Odpowiadasz za bezpieczeństwo odcinka infrastruktury liniowej (kolej/energetyka). Dostajesz zgłoszenie od mieszkańca o dwóch osobach schodzących z nasypu w nocy i o „porzuconym” plecaku.

Wstrzyk 1. Na pobliskiej stacji paliw kamera nagrała te osoby kupujące coś i płacące kartą. **Wstrzyk 2.** W mediach społecznościowych pojawia się nagranie z tego odcinka opublikowane przez anonimowe konto. **Wstrzyk 3.** Analiza pokazuje, że jedna z osób pytała wcześniej pracownika o rozkład pociągów towarowych.

Pytania. Jak zabezpieczasz odcinek i plecak? Które ślady zostawił przeciwnik (karta, CCTV, nagranie, pytania) i jak je zabezpieczyć dla służb? Jak koordynujesz z policją/ABW? Dlaczego amator zostawił tyle śladów?

Punkty nauczania. Amatorstwo wykonawcy = ślad płatniczy, CCTV, publikacja nagrania (faza 4), wcześniejsze pytania (rozpoznanie, grupa B). Rola obrońcy: nie ścigać samemu, lecz zabezpieczyć i przekazać kompletny materiał. Wartość szybkiego, sformalizowanego kanału do służb.

Ćwiczenie 4, „Szara myszka” (na kanwie Dulcewów)

Sytuacja wyjściowa. W otoczeniu chronionej placówki od dwóch lat działa uprzejma właścicielka niewielkiej galerii/firmy, utrzymująca kontakty towarzyskie z personelem, w tym z osobami z dostępem.

Wstrzyk 1. Nigdy nie ma jej na żadnym zdjęciu z wydarzeń, które sama organizuje. **Wstrzyk 2.** Jej „firma” ma znikomą realną działalność, ale dużo podróży zagranicznych. **Wstrzyk 3.** Płaci wyłącznie gotówką, w kwotach niepasujących do skali biznesu.

Pytania. Które wskaźniki grupy D wystąpiły? Dlaczego reakcja „to niemożliwe, taka miła osoba” jest regułą, a nie kontrargumentem? Co robisz, a czego kategorycznie nie (etykietowanie, samodzielne „śledztwo”, pomówienie)? Jak wygląda właściwe, dyskretne zgłoszenie?

Punkty nauczania. Głębokie przykrycie objawia się nie dramatem, lecz nijakością i drobnymi niespójnościami. Zbieg wskaźników D. Zasada zgłoszenia bez etykietowania chroni też osobę potencjalnie niewinną. Rozstrzyga służba, nie ochrona.

Jak prowadzić i podsumować

Prowadzący nie ocenia „dobrze/źle”, lecz naprowadza na: (1) rozpoznanie fazy i grupy wskaźników, (2) zasadę wielu wskaźników, (3) granicę roli, (4) właściwy kanał zgłoszenia. Na koniec każdego ćwiczenia grupa formułuje jedno usprawnienie procedury własnego obiektu. To zamienia ćwiczenie w realną zmianę.

Rozdział 19. Postępowanie po wykryciu, eskalacja i zgłoszenie

Łańcuch reakcji w pięciu krokach

Krok 1, Zauważ i nie zmieniaj sytuacji. Nie dotykaj przedmiotów, nie konfrontuj osób, nie kasuj wiadomości. Zachowaj stan rzeczy i dowody.

Krok 2, Zabezpiecz. Jeśli to przedmiot/przesyłka: strefa, ewakuacja wg procedury, brak kontaktu z przedmiotem. Jeśli to zachowanie: dyskretna obserwacja z zachowaniem roli, bez zaczepiania.

Krok 3, Udokumentuj faktami. Wypełnij właściwą kartę (17). Fakty, godziny, opis czynności, bez etykiet i domysłów o narodowości.

Krok 4, Zgłoś właściwym kanałem. Wewnątrz: przełożony i oficer bezpieczeństwa. Na zewnątrz: policja (tel. alarmowy przy bezpośrednim zagrożeniu) oraz właściwa służba. W Polsce zgłoszenia dotyczące szpiegostwa, sabotażu i dywersji przyjmuje Agencja Bezpieczeństwa Wewnętrznego; przy bezpośrednim zagrożeniu życia lub mienia, najpierw numer alarmowy 112. Organizacja powinna mieć ustalone, imienne punkty kontaktu.

Krok 5, Ogranicz krąg wiedzy. Informacja o wykryciu sama jest wrażliwa. Przekazuj ją wąsko i formalnie, nie w firmowym czacie czy w mediach społecznościowych. Rozgłos może ostrzec przeciwnika, zniszczyć postępowanie i narazić osoby.

> **UWAGA OPSEC: ochrona zgłaszającego i osób trzecich.** Kanał zgłoszenia ma chronić trzy grupy: zgłaszającego (przed odwetem i przed skutkami pomyłki), osobę potencjalnie niewinną (przed pomówieniem) oraz ewentualne działania służb (przed zdekonspirowaniem). Dlatego zgłoszenie idzie do zamkniętego, imiennego kanału, a nie „do wszystkich". To jest praktyczna realizacja postulatu zachowania OPSEC osób podających i odbierających informację o zagrożeniu.

Czego nie robić, katalog błędów

- Nie prowadzić własnego „śledztwa" ani inwigilacji osoby.
- Nie konfrontować i nie zatrzymywać podejrzanego na własną rękę (poza sytuacjami ujęcia obywatelskiego wprost dozwolonymi prawem i bezpiecznymi).
- Nie publikować niczego w sieci, nie „ostrzegać" znajomych.
- Nie etykietować po narodowości, języku, wyglądzie.
- Nie niszczyć i nie „porządkować" dowodów.
- Nie dotykać przedmiotów podejrzanych o właściwości wybuchowe/zapalające.

Rola organizacji między incydentami

Reakcja nie zaczyna się w chwili incydentu, lecz wcześniej: w ustalonych punktach kontaktu ze służbami, w przeszkolonym personelu, w procedurach przyjęć i dostępu, w kulturze zgłaszania wolnej od piętna. Organizacja, która to ma, reaguje o minuty; organizacja, która tego nie ma, traci godziny, a w sabotażu minuty bywają różnicą między wykryciem a szkodą.

Moduł dodatkowy A. Wykrywanie wrogiego rozpoznania wokół placówki (Surveillance Detection, od strony obrońcy)

Moduł napisany w całości z perspektywy obrońcy: uczy rozpoznawać, że ktoś prowadzi rozpoznanie chronionego obiektu. Nie zawiera i celowo pomija techniki prowadzenia obserwacji ani unikania jej przez stronę ofensywną, to jest materiał wykonawczy, którego tu nie ma. Przedmiotem jest wyłącznie *wykrywanie* wrogiego rozpoznania.

Dlaczego rozpoznanie poprzedza atak

Każdy zaplanowany atak, podpalenie, podłożenie ładunku, napaść, sabotaż, poprzedza rozpoznanie celu. Przeciwnik musi ustalić: gdzie są kamery, jak reaguje ochrona, kiedy są dostawy, którędy wjazd, gdzie słabe punkty. Ta faza jest dla obrońcy szansą, bo rozpoznanie zostawia ślady, a między rozpoznaniem a atakiem jest czas. Wykrycie rozpoznania to wykrycie ataku, zanim się wydarzy.

W przypadku placówek dyplomatycznych i obiektów wspierających Ukrainę rozpoznanie bywa dziś prowadzone przez amatorów zwerbowanych przez Telegram (faza 2/3 cyklu), przez drony, a czasem przez wyszkolonych oficerów. Amator zostawia więcej śladów; oficer mniej, ale i on działa w ramach powtarzalnego cyklu rozpoznania, który można rozpoznać.

Cykl wrogiego rozpoznania (do rozpoznania, nie do naśladowania)

Rozpoznanie przeciwnika przebiega zwykle przez powtarzalne czynności: wybór celu, wstępne rozpoznanie z dystansu, rozpoznanie bliskie (fotografowanie, pomiary, testowanie reakcji), próba (np. wejście i wycofanie, „zgubiony” przedmiot) i planowanie ataku. Dla obrońcy każdy z tych etapów ma obserwowalne przejawy: obecność, uwaga skupiona na zabezpieczeniach, dokumentowanie, pytania, testowanie.

Wskaźniki wrogiego rozpoznania

- **Obecność bez celu.** Osoby lub pojazdy przebywające w pobliżu bez wyraźnego powodu, zwłaszcza powtarzalnie i w różnych porach.
- **Uwaga na zabezpieczenia.** Wzrok, telefon lub kamera skierowane na kamery, bramy, posterunki, ogrodzenie, punkty dostępu, nie na to, na co patrzy zwykły przechodzień.
- **Dokumentowanie.** Fotografowanie/filmowanie elementów ochrony; szkicowanie; pomiary; notowanie godzin zmian i dostaw.

- **Pytania.** Wypytywanie personelu, dostawców, sąsiadów o procedury, grafiki, obsadę, drogi, osobiście, telefonicznie, mailowo, przez media społecznościowe.
- **Testowanie reakcji.** Zbliżenie się i wycofanie; wywołanie drobnego incydentu, by zobaczyć, jak reaguje ochrona; „pomyłkowe" wejście.
- **Drony.** Przeloty nad obiektem lub w pobliżu, zwłaszcza powtarzalne.
- **Korelacja z rytmem obiektu.** Obecność skorelowana z dostawami, zmianami ochrony, wizytami, co sugeruje, że ktoś ten rytm bada.

Metoda obrońcy: znać normę, budować pamięć, korelować

Znać normę. Fundamentem jest znajomość normalnego rytmu i normalnego tła obiektu: kto tu bywa, jakie pojazdy, w jakich godzinach. Bez tego nie widać anomalii.

Budować pamięć. Pojedynczy epizod niczego nie znaczy. Dlatego kluczowy jest **rejestr obserwacji** (Karta 1), w którym gromadzi się drobne anomalie z datami. Dopiero przegląd rejestru ujawnia powtarzalność, to samo auto trzeci raz w tygodniu, ta sama osoba przy ogrodzeniu.

Korelować. Zestawianie obserwacji z różnych punktów i zmian, wielu wskaźników naraz. Powtarzalność + uwaga na zabezpieczenia + pytania = obraz rozpoznania, którego żaden pojedynczy element by nie dał.

Wariować to, co widoczne (w granicach roli). Obrońca może utrudniać rozpoznanie, czyniąc reakcje ochrony mniej przewidywalnymi tam, gdzie to dozwolone i bezpieczne, ale to decyzja kierownictwa i procedur, nie improwizacja patrolu.

> **SYGNAŁ OSTRZEGAWCZY.** Najsilniejszym pojedynczym wskaźnikiem wrogiego rozpoznania jest **powtarzalna obecność połączona z uwagą skupioną na zabezpieczeniach**. Turysta fotografuje fasadę; osoba prowadząca rozpoznanie fotografuje kamerę, bramę i posterunek i wraca.

> **UWAGA OPSEC.** Ten moduł nie uczy, jak samemu prowadzić obserwację ani jak jej unikać. Uczy wyłącznie ją wykrywać. Reakcją na wykryte rozpoznanie jest rejestr, korelacja i zgłoszenie, nie konfrontacja i nie kontrśledztwo prowadzone przez ochronę.

Moduł dodatkowy B. Ochrona placówki i reagowanie na podejrzany przedmiot

Moduł praktyczny dla ochrony fizycznej obiektu (w tym placówki dyplomatycznej i węzła logistycznego). Skupia się na tym, co ochrona realnie robi: kontrola dostępu, przyjmowanie przesyłek, reakcja na podejrzany przedmiot, współpraca ze służbami. Wszystko w granicach roli obrońcy.

Warstwy ochrony obiektu

Skuteczna ochrona jest warstwowa: strefa zewnętrzna (otoczenie, podejście, parking), perymetr (ogrodzenie, brama, punkty dostępu), wnętrze (recepcja, strefy kontrolowane) i warstwa proceduralna (dostęp, przesyłki, goście). Wrogie rozpoznanie (moduł A) bada wszystkie warstwy; obrona musi obserwować wszystkie.

Kontrola dostępu, zasady

- Zasada need-to-know wobec informacji o obiekcie (grafiki, obsada, procedury).
- Weryfikacja gości i wykonawców; rejestr wejść; eskorta w strefach wrażliwych.
- Szczególna uwaga na personel miejscowy i podwykonawców w rejonach podwyższonego ryzyka, jako potencjalny cel werbunku (insider risk, Lista kontrolna C).
- Higiena informacji publicznej: przegląd tego, co o obiekcie ujawniają strony, media społecznościowe, zdjęcia, wizytówki.

Przyjmowanie przesyłek, po kampanii paczek 2024

Kampania paczek zapalających uczyniła punkt przyjęć realnym wektorem ataku. Minimalny standard:

- Odseparowany, wyznaczony punkt przyjęć.
- Znajomość profilu normalnych nadawców i przesyłek.
- Weryfikacja nieoczekiwanych przesyłek u adresata przed otwarciem.
- Procedura dla przesyłki bez nadawcy, „testowej” lub z anomalią (waga, zapach, wyciek, dźwięk, temperatura, przewody).
- Jasna ścieżka eskalacji i numer do służb.

Reagowanie na podejrzany przedmiot, protokół 4×NIE + 3×TAK

4×NIE: NIE dotykaj. NIE otwieraj. NIE przemieszczaj. NIE używaj urządzeń radiowych/telefonu tuż przy przedmiocie, jeśli procedura obiektu tak stanowi.

3×TAK: TAK, wyznacz strefę i odsuń ludzi. TAK, powiadom przełożonego i służby. TAK, udokumentuj (Karta 2) i zabezpiecz zapis CCTV.

Rozbrajanie, prześwietlanie i ocena przedmiotu to zadania saperów/służb, nigdy ochrony. Rola ochrony: strefa, ludzie, zgłoszenie, dokumentacja.

Współpraca ze służbami

Placówka i obiekt chroniony powinny mieć ustalone, imienne punkty kontaktu ze służbami (w Polsce m.in. ABW i policja), uzgodnione procedury eskalacji oraz kanał wymiany ostrzeżeń. Wartość tej relacji ujawnia się w kryzysie: obiekt, który wie, do kogo i jak dzwonić, reaguje o minuty; obiekt bez tego traci czas, którego w sabotażu się nie odzyskuje.

> **UWAGA OPSEC.** Także tu obowiązuje wąski krąg wiedzy. Szczegóły zabezpieczeń, luki wykryte podczas ćwiczeń, dane o incydentach, to informacje wrażliwe, których nie umieszcza się w otwartych kanałach. Ich wyciek jest prezentem dla strony prowadzącej rozpoznanie.

Rozdział 20. Test wiedzy i klucz odpowiedzi

Test do wykorzystania po szkoleniu (poziom 1 i 2). 20 pytań; wersja skrócona (1–10) dla poziomu 1. Klucz z komentarzem na końcu.

Pytania

1. Czym jest łączność bezosobowa i jaki problem operacyjny rozwiązuje?
2. Wymień trzy funkcje, które realizowała klasyczna łączność bezosobowa.
3. Dlaczego pojedynczy sygnał ostrzegawczy nie wystarcza do postawienia zarzutu? Jak nazywa się zasada, która to reguluje?
4. Co oznacza termin „agent jednorazowy” i dlaczego jest wygodny dla mocodawcy?
5. Opisz sześć faz cyklu werbunkowego. Między którymi fazami obrona wchodzi najskuteczniej?
6. Dlaczego wymóg sfilmowania działania jest słabością przeciwnika, a nie jego siłą?
7. Wymień trzy „nośniki” ery cyfrowej, które przejęły funkcje dawnej skrzynki i po jednym śladzie, który każdy zostawia.
8. Co zmieniła inwazja z lutego 2022 w sposobie działania rosyjskiego wywiadu w Europie i dlaczego doprowadziło to do fali sabotażu?
9. Podaj protokół reakcji na podejrzany przedmiot (4×NIE + 3×TAK).
10. Komu w Polsce zgłasza się podejrzenie szpiegostwa/sabotażu i jaki numer wybierasz przy bezpośrednim zagrożeniu?
11. Wymień po dwa wskaźniki z każdej z grup A–D (rozdz. 16).
12. Dlaczego reakcja otoczenia „to niemożliwe, taka miła osoba” nie jest kontrargumentem wobec podejrzenia głębokiego przykrycia?
13. Na czym polega zasada zgłoszenia bez etykietowania i kogo chroni?
14. Wskaż najsilniejszy pojedynczy wskaźnik wrogiego rozpoznania obiektu.
15. Dlaczego profilowanie po narodowości/wyglądzie jest nie tylko krzywdzące, ale i nieskuteczne?
16. Jak wyglądał mechanizm wpadki w klasycznych sprawach (Fisher, Ghost Stories) i co to mówi o roli człowieka?
17. Dlaczego amatorstwo współczesnego wykonawcy jest dobrą wiadomością dla obrońcy?
18. Jaka jest granica roli ochrony przy wykryciu zagrożenia? Wymień trzy rzeczy, których ochrona robić nie powinna.
19. Dlaczego wąski krąg wiedzy o incydencie jest częścią bezpieczeństwa, a nie biurokracją?
20. Podaj jedno usprawnienie procedury Twojego obiektu, które wprowadziłbyś po tym szkoleniu.

Klucz odpowiedzi (z komentarzem)

1. Sposób przekazania informacji/rzeczy bez spotkania stron; rozwiązuje problem, że moment spotkania agenta i prowadzącego jest najsłabszym ogniwem, bo daje kontrwywiadowi kadr powiązania.

2. Rozdzielenie tożsamości (kompartmentalizacja), zaprzeczalność, odporność na obserwację.
3. Bo większość wskaźników ma niewinne wyjaśnienia; zasada wielu wskaźników, liczy się zbieg kilku niezależnych sygnałów i odstępstwo od normy.
4. Osoba zwerbowana do jednego zadania, zwykle przez komunikator, często nieświadoma mocodawcy, bez wsparcia po zatrzymaniu; wygodny, bo tani, zaprzeczalny, skalowalny, a jego utrata nic nie kosztuje.
5. Kontakt, Test, Eskalacja, Dowód, Zatrzymanie, Konsekwencje. Najskuteczniej między fazą 1 a 2 (przed pierwszym „niewinnym" zadaniem).
6. Bo nagranie lokalizuje wykonawcę w czasie i miejscu i staje się dowodem w sądzie (por. Leyton).
7. Komunikator (metadane/powiązania), kryptowaluta (łańcuch transakcji), łańcuch kurierski/paczka (nadawca, waga, trasa); dodatkowo dron (sygnatura, operator). Każdy zostawia ślad, którego skrzynka nie zostawiała.
8. Wydalono setki oficerów pod przykryciem dyplomatycznym i zamknięto drogę „turysty" z rosyjskim paszportem; Moskwa przeszła na nielegałów z tożsamością państw trzecich i masowo na lokalnych pośredników jednorazowych, co dało falę taniego, zaprzeczalnego sabotażu.
9. 4×NIE: nie dotykaj, nie otwieraj, nie przemieszczaj, nie używaj radia/telefonu tuż przy (wg procedury). 3×TAK: wyznacz strefę i odsuń ludzi, powiadom przełożonego i służby, udokumentuj i zabezpiecz CCTV.
10. Agencja Bezpieczeństwa Wewnętrznego (oraz policja); przy bezpośrednim zagrożeniu, 112.
11. Odpowiedź otwarta; sprawdź trafność względem rozdz. 16 (np. A: niezamówiona oferta pieniędzy, wymóg filmowania; B: fotografowanie zabezpieczeń, dron; C: przedmiot „nie na miejscu", nietypowa przesyłka; D: unikanie fotografii, gotówka bez pokrycia).
12. Bo głębokie przykrycie objawia się nijakością i drobnymi niespójnościami, a nie „szpiegowskim" dramatem; reakcja niedowierzania otoczenia jest regułą towarzyszącą takim sprawom (por. Krogerowie, Dulcewowie).
13. Zgłaszamy fakty i obserwacje, nie oceny/etykiety; chroni zgłaszającego (przed skutkami pomyłki i odwetem), osobę niewinną (przed pomówieniem) i ewentualne działania służb (przed dekonspiracją).
14. Powtarzalna obecność połączona z uwagą skupioną na zabezpieczeniach (kamery, brama, posterunek).
15. Bo generuje szum, w którym ginie realny sygnał, prowadzi do fałszywych alarmów, jest krzywdzące i często nielegalne; realny wskaźnik to zachowanie, nie tożsamość.
16. Wpadka szła zwykle od człowieka (dezertera/zdrady: Häyhänen, Potiejew) lub od cierpliwej obserwacji, nie od złamania samej łączności; człowiek pozostaje najsłabszym ogniwem.
17. Bo amator nie umie wykrywać obserwacji i zostawia mnóstwo śladów (telefon, płatność, nagranie, publikacja), co ułatwia wykrycie, mimo że bywa groźny przez nieprzewidywalność.
18. Granica: obserwuj–zabezpiecz–zgłoś. Nie: prowadzić własnego śledztwa/inwigilacji; konfrontować/zatrzymywać na własną rękę; publikować/ostrzegać nieformalnie; etykietować; niszczyć dowody; dotykać przedmiotów wybuchowych.
19. Bo informacja o wykryciu jest wrażliwa: jej rozgłos ostrzega przeciwnika, niszczy postępowanie i naraża osoby; wąski, formalny kanał to element ochrony, nie formalność.
20. Odpowiedź otwarta; oceniaj konkretność i wykonalność (np. wdrożenie Listy kontrolnej A w punkcie przyjęć).

Podsumowanie Części III

Moduł szkoleniowy zamienia personel w warstwę czujników. Jego rdzeniem są cztery zasady (anomalia na tle normy, wiele wskaźników, granica roli, zgłoszenie bez etykietowania), sześciofazowy model werbunku, katalog wskaźników w czterech grupach, gotowe karty pracy, dwa moduły dla ochrony obiektu (wykrywanie rozpoznania i reagowanie na przedmiot), cztery ćwiczenia na realnych sprawach oraz test. Całość jest defensywna: uczy wykrywać i zgłaszać, nie wykonywać i wszędzie, gdzie mowa o metodzie przeciwnika, zatrzymuje się przed progiem wykonawczym.

CZĘŚĆ IV. STRONA KONTRWYWIADOWCZA I SYSTEMOWA

Rozdział 21. Jak służby rozbijały siatki

Część III pokazała, co może zrobić pojedyncza organizacja. Ta część pokazuje, jak działa system: służby, prawo, kampanie, odporność infrastruktury. Zaczynamy od metod wykrywania, bo one uzasadniają optymizm części szkoleniowej, przeciwnik, mimo skali, jest wykrywalny.

Sześć dźwigni wykrywania

Analiza spraw z Części II ujawnia sześć powtarzalnych metod, którymi europejskie służby rozbijały siatki.

Wywiad ludzki i dezercja. Najstarsza i wciąż skuteczna dźwignia. Ghost Stories rozbiła zdrada Potiejewa; klasyczne sprawy, Häyhänena i innych. Współcześnie dochodzą źródła wewnątrz siatek proxy oraz współpraca z ukraińskim wywiadem, który rozpracował siatkę zabójstw z 2025–2026.

Obserwacja i praca operacyjna. Cierpliwe dokumentowanie ruchu podejrzanych; w sprawach sabotażu, szybkie zabezpieczenie miejsca i śladów. To dźwignia, którą wspiera warstwa czujników z Części III: wiele spraw zaczęło się od zgłoszenia świadka.

Ślad cyfrowy i płatniczy. Metadane komunikatorów, łańcuch transakcji krypto, dane lokalizacyjne, CCTV, kamery drogowe, rejestry przesyłek. W sprawie Leyton to właśnie splot takich śladów (transmisja nagrania, telefony, zakup paliwa, Signal) domknął sprawę dowodowo.

OSINT i rozpoznawanie twarzy. Rewolucja, którą uosabia Christo Grozev i Bellingcat: publiczne bazy, wycieki, rozpoznawanie twarzy, ślady w mediach społecznościowych. Zdemaskowały nielegałów (Dulcewowie, Kołobowa), których klasyczny kontrwywiad mógłby nie ruszyć latami.

Współpraca międzynarodowa. Wspólne zespoły śledcze przy Eurojust, Europol, wymiana danych. Sprawa paczek zapalających, zespół pięciu państw plus wsparcie kolejnych, pokazuje, że siatka rozpięta na kilka krajów jest ścigana łącznie.

Czujność obywatela i personelu. Zgłoszenia świadków, pracowników, sąsiadów. To najtańsza i najbardziej skalowalna dźwignia i jedyna, na którą wpływ ma każda organizacja. Kampanie uświadamiające (rozdz. 23) mają ją wzmacniać.

Kolejność, która się powtarza

W wielu sprawach widać powtarzalną kolejność: **wskazówka** (od człowieka, OSINT-u lub zgłoszenia) prowadzi do **człowieka**, po czym **obserwacja i ślad cyfrowy** domykają sprawę dowodowo, a **współpraca międzynarodowa** pozwala zwinąć całą siatkę, nie tylko jedno ogniwo. Ta sekwencja tłumaczy, dlaczego warstwa czujników jest tak ważna: dostarcza pierwszej wskazówki, bez której reszta maszyny nie rusza.

Rozdział 21b. Anatomia śledztwa: jak rozplata się sprawę synergiczną

Stan na wrzesień 2026.

Chcę pokazać, jak naprawdę wygląda rozbicie takiej siatki, bo od tego zależy, czy wnioski o obronie mają sens. Będę się trzymał spraw jawnych i publicznych aktów oskarżenia, bo tylko to umiem sprawdzić.

Zacznę od wniosku. Współczesne siatki rzadko wpadają z jednego powodu. Wpadają, bo kilka słabych tropów z różnych warstw zostaje położonych obok siebie. To jest lustrzane odbicie tego, co pisałem o synergii ataku. Atak składa się z warstw, więc i śledztwo składa się z warstw i wygrywa ta strona, która pierwsza zszyje swoje kawałki w całość.

W sprawie paczek zapalających z lipca 2024 widać to jak na dłoni. Paczki nadano z Wilna, zapaliły się w Niemczech, w Polsce i w Wielkiej Brytanii, dwie testowe doszły do USA i Kanady, dwie przechwycono w Amsterdamie. Żadne pojedyncze państwo nie miało pełnego obrazu. Litwa widziała nadanie, Niemcy widziały pożar w Lipsku, Polska swój incydent, Brytyjczycy swój. Dopiero wspólny zespół śledczy przy Eurojust, z Litwą, Polską, Niemcami, Holandią i Wielką Brytanią, przy wsparciu Estonii, Łotwy, Stanów, Kanady i Europolu, złożył to w jedną sprawę i doszedł do liczby dwudziestu dwóch osób wspierających rosyjski wywiad. Proces pięciu oskarżonych ruszył w Wilnie w kwietniu 2026. To jest synergia po stronie obrony: warstwa krajowa zszyta w warstwę międzynarodową.

Druga rzecz, która się powtarza, to że przeciwnik sam produkuje dowody. Model jednorazowy wymaga od wykonawcy nagrania, bo bez dowodu nie ma zapłaty. W sprawie Leyton to nagranie z podpalenia, transmitowane do zleceniodawcy, było jednym z gwoździ. Oceniam, że to jest najgłębsza słabość całego modelu i że przeciwnik długo jej nie usunie, bo wynika nie z niechlujstwa, tylko z braku zaufania między mocodawcą a najętym amatorem. Kto nie ufa wykonawcy, żąda dowodu. Kto żąda dowodu, tworzy materiał do sądu. Ta nieufność jest wpisana w model i pracuje dla nas.

Trzecia warstwa to biały wywiad. Christo Grozev i Bellingcat pokazali, że rozpoznawanie twarzy, wycieki baz danych i cyfrowe okruchy potrafią zdemaskować nawet wyszkolonego nielegała. Marię i Ludwiga ze Słowenii namierzono między innymi dzięki zdjęciu twarzy na stronie szkoły ich dzieci, mimo że para latami unikała fotografowania. Peruwiańską projektantkę z Neapolu, w rzeczywistości oficer GRU, namierzono z pomocą danych z mikroczipa jej kota. Brzmi to jak anegdota, ale to jest właśnie sedno ery danych. W świecie, w którym ślad zostawia dziecko w szkole i kot u weterynarza, rozdzielenie ludzi przestało wystarczać, bo system i tak ich zestawi.

Zwróćmy uwagę na kolejność, bo ona się powtarza od czasów Fishera. Najpierw pojawia się wskazówka, dawniej od dezertera, dziś częściej od świadka, od OSINT-u albo z jednej warstwy technicznej. Wskazówka prowadzi do człowieka. Wokół człowieka domyka się obserwacja i ślad cyfrowy. Współpraca międzynarodowa pozwala zwinąć całą siatkę, a nie jedno ogniwo. Ta sekwencja jest stała. Zmienia się tylko to, skąd przychodzi pierwsza wskazówka i tu jest miejsce, w którym zwykła organizacja realnie coś

zmienia, bo bardzo wiele spraw zaczęło się od tego, że ktoś coś zgłosił.

Czego nie wiem. Nie wiem, ile siatek nie wpadło, bo z definicji ich nie widać. Nie wiem, jak duża część sukcesów to praca operacyjna, a jak duża zwykłe szczęście i błąd amatora, bo akta, które by to rozstrzygnęły, są niejawne. Piszę więc o tym, co widać w wyrokach i pilnuję, żeby nie brać skuteczności za pewnik. Ale to, co widać, wystarcza do jednego twierdzenia. Siatki proxy są wykrywalne, jeśli ktoś zszywa warstwy. I są prawie niewykrywalne, jeśli każdy pilnuje swojej.

Rozdział 21c. Cyber jako jedna z warstw, nie cała wojna

Skoro cała ta książka jest sporem z myśleniem, że liczy się głównie cyber, muszę być sprawiedliwy wobec cyber. Nie twierdzę, że jest nieważny. Twierdzę, że jest jedną warstwą z kilku i że jego siła ujawnia się dopiero w połączeniu z resztą.

Zacznę od faktu. Amerykańska doroczna ocena zagrożeń z 2026 roku wymienia cyberataki w jednym szeregu z dezinformacją, manipulacją rynkiem energii, zastraszaniem militarnym i sabotażem, jako elementy jednej gry w szarej strefie. To jest ważne, bo pokazuje, że nawet w oficjalnej ocenie cyber nie stoi osobno, tylko jest częścią pakietu. Rosyjskie służby, w tym wojskowe, prowadzą operacje cyfrowe wymierzone w infrastrukturę, ale rzadko jako cel sam w sobie. Częściej jako przygotowanie, rozpoznanie albo wzmocnienie działania w innych warstwach.

Pokażę połączenia, bo one są sednem. Werbunek do sabotażu fizycznego idzie kanałem cyfrowym, przez Telegram. Płatność za fizyczne podpalenie idzie kanałem finansowym, w krypto. Rozpoznanie fizycznego obiektu bywa robione cyfrowo, dronem albo z otwartych źródeł, zanim ktokolwiek podejdzie pod bramę. Dezinformacja, czysto cyfrowa, ma osłabić poparcie dla Ukrainy, czyli ten sam cel, który mają fizyczne podpalenia magazynów z pomocą. To jest jeden zamiar realizowany w wielu warstwach naraz. Kto broni tylko warstwy cyfrowej, broni jednej ściany domu, w którym reszta ścian jest z papieru.

Oceniam, że błąd ostatniej dekady polegał nie na tym, że zainwestowaliśmy w cyber, tylko na tym, że zainwestowaliśmy w cyber zamiast, a nie oprócz. Dział bezpieczeństwa informacji urósł, dojrzał, dostał narzędzia i mandat. Ochrona fizyczna w wielu miejscach została tam, gdzie była, traktowana jako koszt i portier. Świadomość personelu, czyli warstwa ludzka, w ogóle bywała pomijana. A przeciwnik uderza dokładnie w te zaniedbane warstwy, bo tam jest najmiększe.

Jest w tym pewna ironia, którą trudno mi pominąć. Włożyliśmy ogromny wysiłek w to, żeby napastnik nie wszedł zdalnie przez sieć i w wielu miejscach udało się to na tyle, że taniej mu wynająć miejscowego, żeby wszedł przez płot z kanistrem. Podniesienie kosztu jednej warstwy przepchnęło przeciwnika do drugiej. To nie jest porażka cyberbezpieczeństwa. To jest dowód, że działa i jednocześnie dowód, że samo nie wystarcza.

Czego nie wiem. Nie wiem, jak rozłożą się proporcje w najbliższych latach, czy przeciwnik wróci mocniej do cyber, gdy fizyczny sabotaż zacznie być zbyt kosztowny w wyrokach, czy odwrotnie. Nie wiem, gdzie jest granica opłacalności, przy której wynajęcie amatora przestaje się Moskwie kalkulować. To zależy od czynników, których z zewnątrz nie zmierzę. Wiem tyle, że dopóki myślimy o cyber i o fizyce jako o dwóch osobnych światach, przeciwnik będzie chodził tam i z powrotem między nimi szybciej, niż my zdążymy przełożyć budżet.

Rozdział 22. Ramy prawne po 2022 roku

Reakcja państw nie ograniczyła się do operacji, objęła też prawo. Rozdział przeglądowo omawia najważniejsze zmiany, bo wyznaczają one ramy, w których działa obrońca i pokazują, że „drobna fucha" jest w istocie ciężkim przestępstwem.

Wielka Brytania, National Security Act 2023

Brytyjska ustawa o bezpieczeństwie narodowym z 2023 roku stworzyła nowoczesne narzędzia ścigania działań na rzecz obcego państwa: przestępstwa przygotowawcze, przyjmowanie korzyści od obcego wywiadu, sabotaż. Sprawa Leyton przyniosła pierwsze skazania z tej ustawy (Earl i Reeves), z wyrokami do 17 lat. Znaczenie precedensowe: pokazała, że nowe prawo pozwala ścigać nawet lokalnego pośrednika działającego przez komunikator jako sprawcę przestępstwa na rzecz obcego państwa.

Niemcy, ściganie i ostrzeganie

Niemcy prowadzą postępowania o szpiegostwo w celu sabotażu (wyrok w Stuttgarcie 2026 za paczki z GPS) oraz o przygotowanie zamachów. Zagrożenie karą sięga wieloletniego więzienia (kampania ostrzegawcza mówi o do 10 lat). Cechą niemieckiego podejścia jest połączenie ścigania z szeroką prewencją informacyjną (rozdz. 23).

Polska, sabotaż, dywersja, szpiegostwo

Polskie organy prowadzą rekordową liczbę postępowań (ponad 60 śledztw szpiegowskich, 82 osoby z zarzutami od 2022 roku wg ABW). Sprawy sabotażu kolejowego (Mika/Puławy) skutkowały zarzutami wobec wykonawców i rosyjskiego organizatora oraz uruchomieniem operacji ochrony infrastruktury. Zaostrzano też przepisy dotyczące dywersji i sabotażu oraz reagowania na drony nad obiektami. Dla firm oznacza to jasny komunikat: współpraca ochrony ze służbami ma dziś oparcie i priorytet.

Poziom Unii Europejskiej, sankcje za zagrożenia hybrydowe

UE zbudowała odrębny reżim sankcji za rosyjskie działania hybrydowe (manipulacja informacją, cyberataki, destabilizacja). W latach 2025–2026 kolejno obejmowano nim osoby i podmioty; reżim przedłużono. To narzędzie polityczno-prawne uzupełnia ściganie karne: uderza w organizatorów i infrastrukturę wpływu, także tam, gdzie sprawców nie da się postawić przed sądem krajowym.

Wniosek dla obrońcy

Ramy prawne po 2022 roku zaostrzyły się i ujednoliciły na tyle, że działania, które kiedyś ginęły jako „zwykły wandalizm” czy „drobne podpalenie”, są dziś ścigane jako przestępstwa na rzecz obcego państwa, z wysokimi wyrokami. To wzmacnia dwa przekazy szkoleniowe: dla potencjalnego rekruta, że ryzyko jest ogromne i realne; dla organizacji, że jej zgłoszenie trafia w system, który potrafi i chce działać.

Rozdział 23. Kampanie uświadamiające jako narzędzie kontrwywiadu

Nowa broń: milion czujników

Najciekawszą innowacją kontrwywiadową ostatnich lat nie jest technologia, lecz zmiana adresata. Skoro przeciwnik werbuje masowo, zwykłych ludzi, przez otwarte platformy, to obroną również stają się zwykli ludzie, ostrzeżeni i wyczuleni. Służby, które dotąd działały w cieniu, zaczęły mówić publicznie.

Przegląd kampanii

Niemcy, „Kein Wegwerf-Agent werden!“ Wspólna kampania BKA, BND, BfV i BAMAD z 2 września 2025 roku. Przekaz: nie daj się zwerbować na „agenta jednorazowego”; ryzykujesz do 10 lat więzienia, często nie wiedząc, dla kogo pracujesz; nie wchodź w kontakt, zgłoś służbom. Sama nazwa jest narzędziem, nadaje zjawisku zapadające w pamięć imię.

Finlandia, SUPO. Publiczny opis sześciofazowego modelu werbunku i jasny przekaz o „jednorazowości” rekruta pozbawionego wsparcia. To materiał, który wprost wykorzystaliśmy w rozdziale 15.

Czechy, BIS. Ujawnienie werbunku migrantów przez Telegram i strategicznego celu (osłabianie spójności społeczeństw, podważanie zaufania do państwa, presja na ograniczenie wsparcia dla Ukrainy). Nazwanie celu odbiera operacjom część mocy.

Polska, ABW. Wznowienie jawnych raportów rocznych po latach przerwy, z twardymi liczbami. Cel wprost deklarowany: budowanie świadomości i zaufania społecznego. Jawność sama w sobie jest tu narzędziem prewencji.

Dlaczego to działa

Kampanie uderzają w model jednorazowy w jego najczulszym punkcie: podaży rekrutów. Jeśli potencjalny wykonawca wie, że „łatwa praca za dobre pieniądze przez Telegram” to najprawdopodobniej faza 1 werbunku kończąca się wieloletnim wyrokiem i porzuceniem przez mocodawcę, pula chętnych się kurczy. A każde zgłoszenie od ostrzeżonego obywatela to pierwsza wskazówka, od której (rozdz. 21) rusza cała maszyna wykrywania.

Dla firmy taka jak polska organizacja ochrony płynie stąd praktyczny wniosek: wewnętrzne szkolenie świadomości (Część III) jest lokalnym odpowiednikiem tych państwowych kampanii i najtańszą inwestycją bezpieczeństwa o najwyższej stopie zwrotu.

Rozdział 24. Odporność organizacji i infrastruktury krytycznej

Od reagowania do odporności

Reagowanie na incydenty jest konieczne, ale niewystarczające. Celem dojrzałej organizacji jest **odporność** (resilience): zdolność do funkcjonowania mimo prób sabotażu i do szybkiego powrotu po incydencie. Odporność buduje się przed atakiem, nie w jego trakcie.

Sześć filarów odporności organizacyjnej

Ludzie. Przeszkolony personel jako warstwa czujników (Część III); kultura zgłaszania wolna od piętna; świadomość insider risk, zwłaszcza wobec personelu miejscowego w rejonach ryzyka.

Procedury. Przyjmowanie przesyłek, kontrola dostępu, reagowanie na podejrzany przedmiot, eskalacja, spisane, przećwiczone, znane personelowi.

Fizyka. Warstwowa ochrona obiektu (moduł B); utwardzenie punktów wrażliwych; przemyślane pokrycie i wykorzystanie CCTV; ochrona przed dronami tam, gdzie to zasadne.

Informacja. Higiena tego, co obiekt ujawnia publicznie; need-to-know wobec grafików i procedur; wąski krąg wiedzy o incydentach i lukach.

Relacje. Ustalone, imienne punkty kontaktu ze służbami (ABW, policja); udział w wymianie ostrzeżeń; współpraca z sąsiednimi obiektami i sektorem.

Ciągłość. Plany na wypadek udanego sabotażu: redundancja, procedury awaryjne, szybkie przywracanie funkcji. W infrastrukturze liniowej (kolej, energetyka, kable) redundancja bywa jedyną realną obroną przed atakiem, którego nie da się w pełni prewencyjnie wykluczyć.

Specyfika infrastruktury rozproszonej

Sprawy Mika/Puławy oraz uszkodzenia kabli bałtyckich pokazują problem infrastruktury rozproszonej: nie da się fizycznie ochronić każdego kilometra toru czy dna morskiego. Odpowiedzią jest połączenie **czujników** (technicznych i ludzkich, mieszkańcy, pracownicy, patrole), **szybkiej reakcji**, **redundancji** oraz **odstraszania** przez wykrywalność i karalność. NATO odpowiedziało na to operacjami Baltic Sentry (kable) i Eastern Sentry (drony), wzmożoną obecnością i szybszą atrybucją. Na poziomie organizacji odpowiednikiem jest gęstsza sieć czujników i krótszy czas reakcji.

Miara dojrzałości

Prosty sprawdzian dojrzałości organizacji: ile czasu upływa od zauważenia anomalii przez szeregowego pracownika do jej dotarcia do właściwej osoby i, w razie potrzeby, do służb? Organizacja odporna mierzy ten czas w minutach. Praca nad jego skróceniem, przez szkolenie, procedury i relacje, jest istotą budowania odporności.

Rozdział 24a. Odporność jako synergia, nie jako suma zabezpieczeń

Wróćmy do synergii, tym razem po stronie obrony, bo to jest praktyczne domknięcie całej książki. Odporność nie jest sumą osobnych zabezpieczeń. Jest ich połączeniem. Można mieć najlepszą ochronę fizyczną, dojrzały dział cyber i przeszkolony personel, a i tak być podatnym, jeśli te trzy rzeczy nie rozmawiają ze sobą. I odwrotnie, można mieć skromne środki w każdej z warstw, a być trudnym celem, jeśli warstwy się zszywają.

Oceniam, że najsłabszym punktem większości organizacji nie jest żadna pojedyncza warstwa, tylko przestrzeń między nimi. Sygnał z recepcji nie dochodzi do ochrony. Notatka ochrony nie dochodzi do osoby, która patrzy na całość. Zgłoszenie z IT o dziwnej wiadomości do pracownika nie spotyka się z obserwacją spod bramy. Każda z tych informacji z osobna jest za słaba, żeby coś uruchomić. Razem układają się w obraz. Przestrzeń między warstwami to jest miejsce, w którym przeciwnik chce, żebyśmy patrzyli osobno.

Praktycznie sprowadza się to do jednej rzeczy, którą nazywam stołem. Musi istnieć miejsce, realne albo proceduralne, na którym spotykają się sygnały ze wszystkich warstw, i osoba, która ma mandat i nawyk je zestawiać. Nie chodzi o nowy dział ani o platformę za miliony. Chodzi o jeden kanał zgłoszeń, o rytm okresowego przeglądu drobnych anomalii i o kogoś, kto ma prawo powiedzieć, że dwie słabe rzeczy z dwóch różnych warstw razem znaczą coś mocnego. W małej organizacji tym stołem jest jedna osoba i cotygodniowe piętnaście minut. W dużej to komórka i procedura. Skala się zmienia, zasada nie.

Wymienię sześć filarów, bo lubię, gdy da się coś policzyć. Ludzie, czyli przeszkolona warstwa czujników i kultura zgłaszania bez piętna. Procedury, spisane i przećwiczone. Fizyka, czyli warstwowa ochrona obiektu. Informacja, czyli higiena tego, co pokazujemy na zewnątrz. Relacje, czyli ustalone kontakty ze służbami i z sąsiednimi obiektami. Ciągłość, czyli redundancja i plan na wypadek, gdy sabotaż się jednak uda. To nie jest lista życzeń. To jest sześć miejsc, w których warto zadać sobie jedno pytanie: czy ta warstwa rozmawia z pozostałymi, czy siedzi w swojej szufladzie.

Czego nie wiem. Nie wiem, gdzie w konkretnej firmie leży próg, za którym zszywanie warstw zamienia się w inwigilację własnych ludzi i zabija zaufanie. Widziałem organizacje, które przeszły ten próg i skończyły z personelem, który przestał cokolwiek zgłaszać. To jest realne ryzyko i nie mam na nie wzoru. Wiem tylko, że odporność stoi na zaufaniu i że stół, który staje się narzędziem podejrzeń, przestaje działać jako stół.

Rozdział 24b. Personel miejscowy i ryzyko wewnętrzne na placówce podwyższonego ryzyka

Ten rozdział piszę z myślą o obiektach w rejonach, gdzie zagrożenie nie jest teorią, w tym o placówkach na Ukrainie i przy jej granicy. Zastrzeżenie na wejściu: to jest materiał o ochronie ludzi, nie o ich podejrzewaniu. Odwracam tu popularny odruch, bo źle ustawiony program insider risk potrafi wyrządzić więcej szkody niż przeciwnik.

Zacznę od faktu. Rosyjski werbunek celuje w personel miejscowy, bo miejscowy ma dostęp, zna rytm obiektu i jest na miejscu, kiedy zewnętrzny agent by nie dotarł. Czeska BIS opisała werbunek migrantów przez Telegram. Model jednorazowy działa najlepiej tam, gdzie są ludzie w trudnej sytuacji i pod presją, a rejon przygraniczny w czasie wojny takich ludzi ma wielu. Oceniam, że na placówce podwyższonego ryzyka personel miejscowy jest jednocześnie największym atutem, bo zna teren i ludzi, i największym wektorem, bo jest celem. Obie rzeczy są prawdziwe naraz i trzeba je trzymać w głowie jednocześnie.

Teraz sedno. Ochrona przed werbunkiem własnych ludzi nie polega na ich śledzeniu. Polega na tym, żeby nie zostawić ich samych w momencie, w którym ktoś próbuje ich złamać. Człowiek w kłopotach finansowych, człowiek z tajemnicą, którą można wykorzystać do szantażu, człowiek, który dostał dziwną ofertę i nie wie, co z nią zrobić. Jeśli taka osoba ma gdzie się zwrócić i wie, że po zgłoszeniu dostanie wsparcie, a nie podejrzenie, to przestaje być łatwym celem. Człowiek, który sam przychodzi i mówi, że ktoś proponował mu pieniądze za informacje o placówce, jest najlepszym czujnikiem, jakiego można mieć. Reakcją na takie zgłoszenie musi być wsparcie i weryfikacja, nigdy natychmiastowe oskarżenie. Bo jeśli raz potraktujemy zgłaszającego jak podejrzanego, następny już nie przyjdzie.

Model, który polecam, brytyjska NPSA nazywa insider risk i sprowadza go do kilku prostych rzeczy. Poufny kanał zgłaszania obaw. Świadomość kadry co do zmian w sytuacji ludzi, ale bez inwigilacji. Reakcja oparta na wsparciu. Świadomość, że celem werbunku bywa właśnie swój. To wszystko brzmi miękko, ale działa twardo, bo uderza w motywację werbunku, a nie w jego skutki.

Powiem też, czego nie robić, bo to jest równie ważne. Nie robić profilowania po narodowości, bo na placówce, gdzie połowa personelu to miejscowi, profilowanie po pochodzeniu to jednocześnie krzywda, nielegalność i utrata najlepszych sojuszników. Nie budować atmosfery podejrzeń, bo ona wypłukuje zaufanie, na którym wszystko stoi. Nie zamieniać programu ochrony ludzi w program ich nadzoru. Granica jest cienka, ale rozpoznawalna: po jednej stronie pytasz, jak pomóc pracownikowi pod presją, po drugiej zbierasz na niego materiał. Pierwsze buduje odporność, drugie ją niszczy.

Czego nie wiem. Nie wiem, jak głęboko sięga werbunek personelu miejscowego w konkretnych miejscach, bo to są dane służb, nie moje. Nie wiem, ilu ludzi, którzy dostali ofertę, jej nie zgłosiło, bo z definicji tego nie widać. Podejrzewam, że więcej, niż byśmy chcieli, i że część z nich milczy nie ze złej woli, tylko ze strachu,

że zostaną potraktowani jak winni. To akurat jest w zasięgu naszej decyzji. Jeśli zgłoszenie boli mniej niż milczenie, ludzie będą zgłaszać.

Rozdział 24c. Dron nad obiektem: rozpoznanie i reakcja

Drony zasługują na osobny rozdział, bo są tym miejscem, w którym rozpoznanie i atak najwyraźniej się zlewają, i bo to jest obszar, w którym akurat coś wiem z roboty. Zastrzeżenie jak zwykle: piszę o rozpoznawaniu i reagowaniu na cudze drony, nie o tym, jak drona prowadzić czy jak omijać detekcję. To druga strona i nie moja.

Wniosek na wejściu. Dron nad obiektem wrażliwym rzadko jest przypadkiem i prawie nigdy nie jest tylko obserwacją. Fala naruszeń przestrzeni powietrznej nad europejskimi obiektami w latach 2025 i 2026, drony nad lotniskami, bazami, portami, a w sierpniu 2026 dron z ładunkiem wykryty przy samolocie cargo na lotnisku Lipsk-Halle, pokazała, że ten sam nośnik, który dziś fotografuje, jutro może przenieść ładunek. Niemiecki minister spraw wewnętrznych nazwał tamten incydent możliwym scenariuszem ataku hybrydowego. Dlatego drona nad obiektem traktuję jako wczesną fazę potencjalnego ataku, nie jako ciekawostkę.

Rozpoznanie od strony obrońcy zaczyna się od tego samego, co wszystko inne w tej książce: od znajomości normy. Nad wieloma obiektami drony latają legalnie i niewinnie, rolnicze, budowlane, hobbystyczne. Sygnałem nie jest sam dron, tylko dron zachowujący się nie tak: powtarzalne przeloty nad tym samym punktem, zawisanie nad wejściami i posterunkami, loty w nietypowych porach, korelacja z rytmem obiektu, na przykład z dostawami albo zmianami ochrony. Pojedynczy przelot to zwykle nic. Trzeci przelot nad tym samym punktem w tym samym tygodniu to już wzorzec, który idzie do rejestru i do zgłoszenia.

Reakcja mieści się w granicy roli, i tu muszę być twardy, bo to jest obszar, w którym łatwo zrobić głupstwo. Ochrona obiektu nie strąca dronów i nie zakłóca ich na własną rękę. W większości jurysdykcji jest to nielegalne, bywa niebezpieczne, a spadający dron z ładunkiem to gorszy problem niż dron w locie. Rola ochrony to: odnotować, udokumentować, powiadomić i chronić ludzi. Zejście personelu z otwartej przestrzeni, jeśli dron zachowuje się groźnie. Zapis czasu, kierunku, wysokości, zachowania. Powiadomienie właściwych służb, bo przeciwdziałanie dronom to ich domena i domena wyspecjalizowanych systemów, nie portiera z lornetką. Wariowanie tego, co widoczne, w granicach procedury, żeby utrudnić rozpoznanie, ale to decyzja kierownictwa, nie improwizacja.

Czego nie wiem. Nie wiem, jaka część przelotów nad polskimi obiektami to świadome rozpoznanie, a jaka zwykły ruch, bo bez danych z detekcji tego się nie rozdzieli, a te dane rzadko są jawne. Nie wiem, jak szybko tanie systemy detekcji staną się standardem na obiektach cywilnych, bo to zależy od kosztów utrzymania po roku, których dla wielu wdrożeń nie znam. Oceniam, na podstawie własnej roboty przy detekcji na poziomie TRL4, że sieć tanich czujników pokryje newralgiczne punkty szybciej niż drogie radary, ale to jest ocena z jednego obszaru, nie fakt, i uczciwie ją tak oznaczam.

Rozdział 25. Prognoza i wnioski

Dokąd to zmierza

Na podstawie tego, co wiadomo do połowy 2026 roku, można sformułować kilka ostrożnych prognoz.

Kampania hybrydowa nie osłabnie. Ośrodki analityczne (Carnegie, GLOBSEC) przewidują eskalację, a nie wygaszenie. Dopóki trwa wojna i dopóki Moskwa uznaje sabotaż za tani, zaprzeczalny sposób nacisku, presja będzie się utrzymywać, a Polska pozostanie w pierwszej linii.

Model jednorazowy pozostanie dominujący, ale będzie ewoluował. Werbunek przez komunikatory, płatności w krypto, wykorzystanie łańcucha kurierskiego i dronów, to trwały repertuar. Będzie się doskonalił (lepsza kompartmentalizacja, mniej śladów), ale jego fundamentalne słabości, amatorstwo wykonawcy, ślad cyfrowy, wymóg dowodu, pozostaną.

Klasyczny nielegał nie zniknie, choć będzie coraz rzadszy i coraz droższy. Samo źródło Walkera przyznaje: budowa legend w erze biometrii jest coraz trudniejsza, ale „zapotrzebowanie pozostaje ogromne". Będziemy więc widzieć dalsze demaskacje pojedynczych, głęboko ukrytych agentów, zwykle dzięki OSINT-owi i biometrii.

Granica między rozpoznaniem a atakiem będzie się zacierać. Dron, który dziś rozpoznaje, jutro może przenosić ładunek (incydent w Lipsku 2026). To wymusi traktowanie rozpoznania jako wczesnej fazy ataku, a nie odrębnego, łagodniejszego zjawiska.

Trzy wnioski końcowe

Pierwszy: przewaga wróciła do obrońcy, jeśli obrońca ją wykorzysta. Przez dekady klasyczna łączność bezosobowa dawała przewagę stronie ofensywnej, bo była niemal nie do złamania od zewnątrz. Era danych odwróciła ten układ: przeciwnik, przechodząc na model masowy i cyfrowy, zyskał skalę, ale utracił niewidzialność. Każdy nowy nośnik zostawia ślad. To realna, strukturalna przewaga obrońcy, pod warunkiem, że ma on warstwę czujników zdolną wychwycić pierwszą wskazówkę.

Drugi: najważniejszym czujnikiem jest przeszkolony człowiek. Nie technologia, nie prawo, nie sankcje, choć wszystkie są potrzebne, lecz ostrzeżony, wyczulony pracownik, który rozpoznaje sygnał i wie, jak go zgłosić. To dlatego państwa przeszły od milczenia do publicznych kampanii, a organizacje powinny pójść tą samą drogą wewnętrznie. Część III tego opracowania jest właśnie taką kampanią w miniaturze.

Trzeci: obrona ma granicę, której nie wolno przekroczyć i to jest jej siła, nie słabość. Rola obrońcy kończy się na: rozpoznaj, zabezpiecz, zgłoś. Nie na kontrśledztwie, nie na inwigilacji, nie na odtwarzaniu metod przeciwnika. Ta granica chroni dowody, chroni osoby niewinne, chroni samych zgłaszających i chroni działania służb. Jest też linią, przy której zatrzymuje się to opracowanie: opisaliśmy, jak przeciwnik działa i jak go rozpoznać, ale nie, jak go naśladować. Bo skuteczna obrona nie wymaga umiejętności ataku. Wymaga

uwagi, procedury i dyscypliny. I te trzy rzeczy są w zasięgu każdej organizacji, która zdecyduje się je zbudować.

Podsumowanie Części IV

System obrony ma cztery warstwy: służby (sześć dźwigni wykrywania, z pierwszą wskazówką od czujników), prawo (zaostrzone i ujednolicone po 2022 roku, czyniące „drobną fuchę” ciężkim przestępstwem), kampanie uświadamiające (milion czujników uderzający w podaż rekrutów) oraz odporność organizacji i infrastruktury (sześć filarów, krótki czas reakcji, redundancja). Wszystkie cztery warstwy schodzą się w jednym punkcie: przeszkolonym człowieku, który rozpoznaje anomalię i zgłasza ją we właściwy sposób. To jest zwornik całego opracowania.

CZĘŚĆ V. PRZEWODNIK METODYCZNY DLA PROWADZĄCEGO SZKOLENIE

Rozdział 26. Jak przygotować i poprowadzić szkolenie

Część V jest praktycznym przewodnikiem dla osoby, która ma to szkolenie przeprowadzić: oficera bezpieczeństwa, trenera wewnętrznego, koordynatora ochrony. Zawiera plany sesji, scenariusze slajdów, dodatkowe ćwiczenia, materiały do rozdania i wskazówki dydaktyczne. Można ją traktować jako gotowy zestaw narzędzi.

Zasada nadrzędna: uczymy nawyku, nie wiedzy

Cel szkolenia nie polega na tym, by uczestnik zapamiętał definicje. Polega na tym, by w realnej sytuacji, gdy zobaczy anomalię, zadziałał odruchowo we właściwy sposób: rozpoznał, zabezpieczył, zgłosił, nie przekroczył roli. To jest nauka nawyku, a nawyku nie buduje się wykładem. Buduje się go powtarzaniem, ćwiczeniem i konkretem. Dlatego proporcja czasu powinna wyraźnie faworyzować część warsztatową nad wykładową: reguła kciuka to najwyżej jedna trzecia czasu na teorię, co najmniej dwie trzecie na ćwiczenia, dyskusję i odgrywanie sytuacji.

Zasada realizmu: pracujemy na prawdziwych sprawach

Uczestnicy, zwłaszcza doświadczeni, słusznie nie ufają abstrakcji. Dlatego całe szkolenie osadzone jest na sprawach rzeczywistych, publicznie udokumentowanych: Leyton, paczki DHL, Mika i Puławy, siatka litewska, Dulcewowie. Prowadzący powinien znać te sprawy na tyle dobrze, by odpowiadać na pytania i wiązać każdą regułę z konkretem. „Zasada wielu wskaźników” jest abstrakcją; „w sprawie Leyton dopiero zbieg nagrania, śladu telefonu i zakupu paliwa domknął sprawę” jest konkretem, który zapada w pamięć.

Zasada bezpieczeństwa przekazu: linia obronna, nie ofensywna

Prowadzący musi utrzymać tę samą linię, która obowiązuje w całym opracowaniu. Szkolenie uczy rozpoznawać i reagować, nie uczy prowadzić operacji. Jeśli w trakcie zajęć padnie pytanie „a jak właściwie zakłada się taką skrzynkę” albo „jak ominąć monitoring”, właściwą odpowiedzią jest spokojne wyjaśnienie, że to wiedza wykonawcza, która nie jest przedmiotem tego szkolenia, bo obrona jej nie potrzebuje i przekierowanie na pytanie „jak byśmy to wykryli”. Ta postawa sama w sobie jest elementem kultury bezpieczeństwa, którą budujemy.

Cztery komunikaty, które muszą zostać w głowie

Jeśli po szkoleniu uczestnik ma zapamiętać tylko cztery rzeczy, powinny to być:

1. **Anomalia na tle normy.** Znaj rytm swojego obiektu; reaguj na odstępstwo.
2. **Wiele wskaźników, nie jeden.** Sumuj, nie oskarżaj pochopnie.
3. **Granica roli: rozpoznaj, zabezpiecz, zgłoś.** Nie ścigaj, nie konfrontuj, nie dotykaj.
4. **Zgłoszenie bez etykietowania, wąskim kanałem.** Fakty, nie oceny; do właściwej osoby, nie do wszystkich.

Wszystko inne jest rozwinięciem tych czterech zdań. Prowadzący powinien wracać do nich wielokrotnie i zamknąć nimi szkolenie.

Rozdział 27. Plany sesji dla trzech poziomów odbiorców

Sesja dla poziomu 1, cały personel (90 minut)

Cel: każdy pracownik rozpoznaje sygnał werbunku i podejrzanej sytuacji oraz wie, jak zgłosić.

- **0–10 min. Wprowadzenie i „dlaczego to nas dotyczy”.** Krótko: Polska w pierwszej linii, cele cywilne, przykład Mika/Puławy. Cel: przełamać poczucie „to nie o nas”.
- **10–30 min. Jak wygląda werbunek.** Sześć faz cyklu (rozdz. 15) na przykładzie „łatwej pracy z Telegrama”. Nacisk na fazę 1–2 i na to, że ofiara często nie wie, dla kogo pracuje.
- **30–45 min. Katalog sygnałów, grupy A i C.** Konkretne przykłady; ćwiczenie „niewinne czy podejrzane?” (rozdz. 28).
- **45–60 min. Co robić.** Łańcuch reakcji w pięciu krokach (rozdz. 19); protokół podejrzanego przedmiotu (4×NIE + 3×TAK); kanał zgłoszenia w naszej organizacji.
- **60–80 min. Ćwiczenie.** Jedno krótkie ćwiczenie sytuacyjne (np. „dostajesz taką wiadomość, co robisz?“).
- **80–90 min. Test skrócony (1–10) i cztery komunikaty na koniec.**

Sesja dla poziomu 2, ochrona i oficerowie bezpieczeństwa (1 dzień)

Cel: personel ochrony rozpoznaje wrogie rozpoznanie i podejrzane przedmioty, prowadzi rejestr, właściwie eskaluje.

- **Blok I (rano, 90 min). Zagrożenie i mechanizm.** Część II w pigułce: od nielegała do agenta jednorazowego; sześć faz; nośniki cyfrowe. Dużo konkretu ze spraw.
- **Blok II (rano, 90 min). Rozpoznawanie.** Katalog wskaźników (wszystkie grupy); moduł wykrywania wrogiego rozpoznania (moduł A); praca z Kartą 1 (rejestr obserwacji).
- **Przerwa.**
- **Blok III (po południu, 90 min). Reagowanie.** Moduł ochrony obiektu (moduł B); protokół przedmiotu; przyjmowanie przesyłek; łańcuch reakcji; granica roli.
- **Blok IV (po południu, 90 min). Warsztat.** Dwa ćwiczenia tabletop (rozdz. 18 lub 28); po każdym, jedno usprawnienie procedury własnego obiektu.
- **Zamknięcie (30 min). Test pełny (1–20), omówienie, cztery komunikaty.**

Sesja dla poziomu 3, kadra kierownicza i analitycy (pół dnia)

Cel: decydenci rozumieją zagrożenie na tyle, by inwestować w odporność, ustalać relacje ze służbami i ustawiać procedury.

- **Blok I (60 min). Obraz strategiczny.** Część II i IV w skrócie: skala, geografia, prognoza; co to znaczy dla naszej organizacji.
- **Blok II (60 min). Sześć filarów odporności (rozdz. 24).** Samoocena organizacji względem każdego filara.
- **Blok III (60 min). Ćwiczenie decyzyjne.** Jedno tabletop z perspektywy zarządczej: nie „co robi patrol", lecz „jak reagujemy jako organizacja, kogo zawiadamiamy, jak komunikujemy".
- **Zamknięcie (30 min). Plan działania: trzy rzeczy, które wdrożymy w 30 dni.**

Wskazówki logistyczne

Grupy warsztatowe najlepiej działają w rozmiarze 6–12 osób. Ćwiczenia tabletop wymagają prowadzącego, który zna sprawy i pilnuje, by dyskusja szła w stronę rozpoznania i reakcji, a nie „gdybania". Sala powinna umożliwiać pracę w małych zespołach. Materiały do rozdania (karty z rozdz. 17, karta zbiorcza z Dodatku C) warto wydrukować i zostawić uczestnikom, to zwiększa szansę, że wiedza przełoży się na praktykę.

Rozdział 28. Dodatkowe ćwiczenia i materiały warsztatowe

Ćwiczenie „niewinne czy podejrzane?” (rozgrzewka, 15 min)

Prowadzący czyta krótkie sytuacje; uczestnicy decydują: niewinne, podejrzane, czy „zależy, potrzebuję więcej wskaźników”. Celem jest wyćwiczenie zasady wielu wskaźników i odruchu nie-oskarżania na podstawie jednego sygnału.

Przykładowe sytuacje: - Turysta fotografuje zabytkowy budynek obok chronionego obiektu. *(Zwykle niewinne; podejrzane dopiero, gdy fotografuje kamery i wraca.)* - Nowy dostawca pyta o godziny przyjęć towaru. *(Zwykle niewinne; kontekst rozstrzyga.)* - Ktoś oferuje pracownikowi 500 euro za zdjęcia bramy przez Telegram. *(Podejrzane, faza 1/2 werbunku, zgłoś.)* - Cudzoziemiec ma silny akcent. *(Niewinne; sam akcent nigdy nie jest wskaźnikiem.)* - Ta sama osoba trzeci raz w tygodniu stoi przy ogrodzeniu z telefonem skierowanym na posterunek. *(Podejrzane, powtarzalność + uwaga na zabezpieczenia.)* - Nieoczekiwana paczka bez nadawcy, cięższa niż deklarowana zawartość. *(Podejrzane, procedura przedmiotu.)*

Punkt nauczania: większość pojedynczych sygnałów jest niewinna; dopiero zbieg i powtarzalność uzasadniają zgłoszenie. Jednocześnie niektóre sygnały (oferta werbunku, podejrzana paczka) uzasadniają reakcję same, bo dotyczą czynu, nie tożsamości.

Ćwiczenie tabletop 5, Placówka dyplomatyczna (dla poziomu 2/3)

Sytuacja wyjściowa. Odpowiadasz za bezpieczeństwo placówki. Od trzech tygodni personel recepcji odnotowuje powtarzające się telefony z pytaniami o godziny pracy, obsadę i procedury wejścia; rozmówca za każdym razem się rozłącza, gdy pada prośba o przedstawienie się.

Wstrzyk 1. Ochrona zauważa zaparkowany naprzeciw wejścia samochód, w którym ktoś siedzi przez dłuższy czas w różne dni; przy zbliżeniu patrolu odjeżdża. **Wstrzyk 2.** Miejscowy pracownik zgłasza, że zaczepił go nieznajomy z ofertą „dodatkowego zarobku” za informacje o rozkładzie dnia placówki. **Wstrzyk 3.** W mediach społecznościowych pojawia się zdjęcie wejścia placówki zrobione z ulicy, opublikowane przez anonimowe konto.

Pytania. Które grupy wskaźników wystąpiły (A, B)? Jak dokumentujesz (Karta 1)? Co robisz ze zgłoszeniem miejscowego pracownika (insider risk, ale też potencjalna ofiara werbunku)? Jak i komu eskalujesz? Jak chronisz miejscowego pracownika przed odwetem i przed pochopnym oskarżeniem? Czego nie robisz?

Punkty nauczania. To klasyczny wzorzec wrogiego rozpoznania placówki. Reakcja: rejestr, korelacja, zgłoszenie właściwym kanałem, ochrona zgłaszającego. Miejscowy pracownik, który sam zgłosił ofertę, jest sojusznikiem, reakcją jest wsparcie i weryfikacja, nie podejrzenie. Zgłoszenie idzie wąskim, imiennym kanałem, nie do ogółu personelu.

Ćwiczenie tabletop 6, Węzeł logistyczny wsparcia (dla poziomu 2)

Sytuacja wyjściowa. Chronisz centrum przeładunkowe, przez które przechodzą m.in. transporty pomocy. Kierowca zgłasza, że na parkingu ktoś przyczepił do naczepy niewielkie urządzenie, którego wcześniej nie było.

Wstrzyk 1. Urządzenie przypomina nadajnik; kierowca zdążył je dotknąć, zanim zgłosił. **Wstrzyk 2.** Analiza nagrań pokazuje osobę, która krążyła po parkingu poprzedniego wieczoru, zaglądając pod naczepy. **Wstrzyk 3.** Podobne zgłoszenie napłynęło z sąsiedniego terminala.

Pytania. Jak zabezpieczasz urządzenie i pojazd, skoro kierowca już go dotknął? Które ślady zostawił przeciwnik? Jak koordynujesz z sąsiednim terminalem i ze służbami? Jak zmienisz procedurę kontroli pojazdów po tym zdarzeniu?

Punkty nauczania. Nadajnik na pojeździe to rozpoznanie trasy (wariant „paczka z GPS” przeniesiony na pojazd). Powtarzalność między terminalami = wzorzec, nie przypadek. Wartość wymiany informacji między obiektami. Procedura kontroli pojazdów jako usprawnienie.

Karta uczestnika, „Moje trzy zobowiązania”

Na koniec każdej sesji uczestnik wypełnia i zabiera kartę:

- Jedna rzecz, którą od jutra będę robić inaczej: ____
- Jeden sygnał, którego wcześniej bym nie zauważył, a teraz zauważę: ____
- Do kogo dokładnie zgłoszę, jeśli coś zauważę (imię/funkcja/numer): ____

Ta prosta karta zamienia szkolenie w zobowiązanie i wielokrotnie zwiększa szansę na realną zmianę zachowania.

Rozdział 29. Mity i fakty oraz najczęstsze pytania uczestników

Rozdział zbiera powtarzające się nieporozumienia i trudne pytania, które padają na szkoleniach. Prowadzący może wykorzystać go jako gotowe odpowiedzi.

Mity i fakty

Mit: „Szpieg wygląda i zachowuje się jak szpieg”. Fakt: głębokie przykrycie objawia się nijakością, uprzejmością i gładką biografią, a nie dramatem. Reakcja otoczenia demaskowanych nielegałów niemal zawsze brzmi „to niemożliwe, tacy mili ludzie” (Krogerowie, Dulcewowie). Zwyczajność jest kamuflażem.

Mit: „To zagrożenie dotyczy tylko wojska i rządu”. Fakt: cele są rozproszone i w dużej mierze cywilne, magazyny, logistyka, kolej, energetyka, a nawet centra handlowe. Raport ABW wskazuje na gotowość przeciwnika do ofiar cywilnych. „Cywilny” charakter obiektu nie wyłącza go z kręgu celów.

Mit: „Prawdziwy sabotaż robią wyszkoleni profesjonaliści”. Fakt: coraz częściej robią go amatorzy zwerbowani przez czat za kilka tysięcy euro, nieświadomi, dla kogo pracują. To ich amatorstwo czyni ich groźnymi (nieprzewidywalność), ale i wykrywalnymi (ślady).

Mit: „Jak zauważę coś podejrzanego, powinienem sam sprawdzić, zanim zaalarmuję”. Fakt: samodzielne „śledztwo” niszczy dowody, naraża osobę i przekracza rolę. Właściwa kolejność to rozpoznaj–zabezpiecz–zgłoś, a weryfikację prowadzą powołane do tego osoby i służby.

Mit: „Zgłoszenie kogoś niewinnego to katastrofa, więc lepiej nie zgłaszać”. Fakt: zgłoszenie faktów bez etykiet nie jest oskarżeniem. Zasada wielu wskaźników i wąski kanał chronią osobę niewinną. Niezgłoszenie realnego sygnału jest znacznie groźniejsze niż zgłoszenie, które okaże się nieuzasadnione.

Mit: „Kryptowaluty i Telegram są niewykrywalne”. Fakt: treść bywa szyfrowana, ale metadane, powiązania, łańcuch transakcji i urządzenia zostawiają ślady, które służby potrafią rozpracować, zwłaszcza gdy wykonawca jest amatorem.

Najczęstsze pytania

„Czy nie popadniemy w paranoję, podejrzewając wszystkich?“ Nie, jeśli trzymamy się zasady wielu wskaźników i zasady anomalii na tle normy. Nie chodzi o podejrzewanie wszystkich, lecz o zauważanie odstępstw od znanej normy i sumowanie sygnałów. Paranoja to reagowanie na pojedynczy sygnał; profesjonalizm to cierpliwe budowanie obrazu.

„Co, jeśli zgłoszę, a to była pomyłka?“ To normalne i akceptowalne. System jest zaprojektowany tak, by weryfikacja odbywała się na właściwym poziomie. Twoim zadaniem jest przekazać rzetelną obserwację, nie

postawić diagnozę. Dobre zgłoszenie faktów nigdy nie jest błędem.

„Czy mogę zatrzymać podejrzaną osobę?“ Co do zasady nie, to nie jest rola ochrony poza wąskimi, prawnie dozwolonymi i bezpiecznymi sytuacjami. Twoja rola to obserwacja, zabezpieczenie i zgłoszenie. Zatrzymanie na własną rękę naraża ciebie, może być nielegalne i niszczy postępowanie.

„A jeśli to ktoś z naszych?“ Werbunek własnego personelu, zwłaszcza miejscowego w rejonach ryzyka, jest realnym wektorem. Reakcją nie jest oskarżenie, lecz odnotowanie sygnałów i zgłoszenie właściwym, poufnym kanałem, zgodnie z modelem insider risk. Osoba, która sama zgłasza próbę werbunku, jest sojusznikiem, nie podejrzanym.

„Po co uczyć się o martwych skrzynkach, skoro to już przeszłość?“ Bo sposób myślenia, szukanie anomalii, sumowanie wskaźników, nieufność wobec „wymuszonej niewinności”, jest przenaszalny na współczesne zagrożenia. A klasyczne metody nie zniknęły całkowicie; wracają przy przekazie pieniędzy i sprzętu w siatkach.

„Czy to szkolenie uczy nas szpiegować?“ Nie. Uczy wykrywać i reagować. Świadomie nie zawiera treści wykonawczych. Skuteczna obrona nie wymaga umiejętności ataku, wymaga uwagi, procedury i dyscypliny.

Rozdział 30. OPSEC obrońcy: jak nie oddać przeciwnikowi tego, czego sam szuka

Ten rozdział jest o bezpieczeństwie operacyjnym, ale patrzę na nie z jednej strony: obrońcy. Nie piszę, jak agent chroni swoją operację. Piszę, jak organizacja i jej ludzie chronią to, po co przeciwnik przychodzi. To jest ta sama zasada, którą stosuję we wszystkim, co robię. Analiza nie jest instrukcją, a OPSEC obrońcy to nie lustro OPSEC-u napastnika, tylko osobna dyscyplina.

Wniosek stawiam na wejściu. Większość informacji, których potrzebuje przeciwnik, żeby zaplanować rozpoznanie albo sabotaż, oddajemy mu sami. Grafiki, obsada, rozkłady dostaw, zdjęcia z firmowych profili, wizytówki na konferencjach, zbyt gadatliwe strony internetowe. Rozpoznanie zaczyna się od tego, co jawne i dopiero potem schodzi na miejsce. OPSEC obrońcy polega na tym, żeby jawnego było mniej, a to, co zostaje, mówiło mniej.

Co przeciwnik zbiera, zanim w ogóle się pojawi

Zanim ktokolwiek stanie pod ogrodzeniem, wie już sporo. Wie z sieci, jak wygląda wejście, bo ktoś wrzucił zdjęcie z eventu. Wie, kto odpowiada za ochronę, bo ktoś podał to na LinkedIn. Wie, kiedy przyjeżdżają dostawy, bo o to samo można zapytać przez telefon i zwykle dostaje się odpowiedź. To nie jest teoria. W sprawie słoweńskich nielegałów legendą przykrycia była firma, która głównie jeździła na branżowe konferencje, w tym na dużą imprezę cyberbezpieczeństwa. Ludzie sami przychodzą tam, gdzie jest dostęp i sami o tym opowiadają.

Oceniam, że dla większości chronionych obiektów największy wyciek nie idzie przez mur, tylko przez otwarte kanały własnej organizacji. To dobra wiadomość, bo akurat to jest w zasięgu decyzji, nie budżetu.

Higiena informacji jawnej

Pierwsza rzecz to przegląd własnego śladu. Co o obiekcie mówią strona internetowa, profile w mediach społecznościowych, zdjęcia z wydarzeń, oferty pracy, wizytówki, tabliczki. Oferta pracy na stanowisko w ochronie potrafi zdradzić system zmian. Zdjęcie z firmowej wigilii potrafi pokazać wnętrze recepcji i identyfikatory. Nie chodzi o paranoję i zamykanie się na świat, tylko o świadomą decyzję, co pokazujemy i po co.

Zasada, którą polecam, jest prosta: informacje o zabezpieczeniach, grafikach, obsadzie i procedurach traktujemy według reguły need-to-know, czyli dostaje je ten, kto ich potrzebuje do pracy i nikt więcej. To nie jest tajność dla samej tajności. To odbieranie przeciwnikowi darmowego rozpoznania.

Ochrona ludzi

Najcenniejsze, co ma organizacja, to ludzie i to oni są celem werbunku. Personel miejscowy w rejonie podwyższonego ryzyka, pracownik w kłopotach finansowych, ktoś podatny na szantaż. OPSEC obrońcy obejmuje więc nie tylko dane, ale i ludzi: kultura, w której pracownik w tarapatach ma gdzie się zwrócić, a zgłoszenie próby werbunku spotyka się ze wsparciem, a nie z podejrzeniem, jest realną barierą. Człowiek zostawiony sam z szantażem jest podatny. Człowiek, który wie, że po zgłoszeniu dostanie pomoc, nie ma czym być szantażowany.

Odwracam tu popularny odruch. Model insider risk nie jest o inwigilowaniu własnych ludzi. Jest o tym, żeby ich nie zostawić samych w momencie, w którym ktoś próbuje ich złamać. To jest OPSEC prowadzony przez zaufanie, nie przez podejrzenie i oceniam, że działa lepiej, bo ludzie sami przynoszą sygnały, zamiast je ukrywać.

Ochrona kanału zgłoszeń

Jest rzecz, o której łatwo zapomnieć: sama informacja o zagrożeniu jest wrażliwa. Jeśli ktoś zauważy rozpoznanie obiektu i napisze o tym na firmowym czacie dostępnym dla stu osób, to właśnie oddał przeciwnikowi wiedzę, że został zauważony i podał ją dalej, niż trzeba. Dlatego zgłoszenie idzie wąskim, imiennym kanałem do konkretnej osoby, a nie do ogółu. To chroni trzy strony naraz. Chroni zgłaszającego przed odwetem i przed skutkami pomyłki. Chroni osobę potencjalnie niewinną przed pomówieniem, które rozejdzie się szybciej, niż da się je odwołać. I chroni ewentualne działania służb, bo rozgłos potrafi spłoszyć sprawę, zanim dojdzie do zatrzymania.

To jest praktyczne znaczenie prośby, którą słyszę od ludzi z tej branży najczęściej: zachować OPSEC osób, które podają i odbierają informację. Nie chodzi o tajemniczość dla efektu. Chodzi o to, że wąski kanał ratuje ludzi i ratuje sprawy.

Higiena cyfrowa bez magii

Nie obiecuję cudów technicznych i nie sprzedaję narzędzi. Kilka rzeczy jest jednak tanich i działa. Rozdzielenie kont prywatnych i służbowych. Ostrożność z tym, co personel publikuje o pracy. Świadomość, że komunikator szyfruje treść, ale nie chowa faktu i metadanych kontaktu. Świadomość, że zdjęcie z telefonu niesie czas i często lokalizację. To nie jest wiedza tajemna, to higiena, a większość wycieków bierze się z jej braku, nie z genialnego przeciwnika.

Piszę to ostrożnie, bo tu przebiega granica, której pilnuję. Nie opisuję, jak omijać wykrycie, jak konfigurować rzeczy pod nieuchwytność ani jak działać, żeby nie zostawić śladu. To byłby OPSEC napastnika, a ta książka jest po drugiej stronie. Higiena obrońcy kończy się tam, gdzie zaczyna instrukcja dla kogoś, kto chce zniknąć.

Czego nie wiem

Nie wiem, ile z wycieków, które widuję, jest przypadkiem, a ile świadomym rozpoznaniem. Nie wiem, jak głęboko sięga werbunek personelu miejscowego w konkretnych miejscach, bo to są dane służb, nie moje. Nie wiem, gdzie dokładnie leży granica, za którą dobra higiena informacji zamienia się w paraliż organizacji, bo to zależy od obiektu i od ryzyka. Zostawiam te luki widoczne, bo tak wolę, niż udawać, że mam całą mapę.

Jedno oceniam z przekonaniem. OPSEC obrońcy to w dziewięciu przypadkach na dziesięć nie technika, tylko dyscyplina i kultura. Mniej pokazywać, wąsko zgłaszać, nie zostawiać ludzi samych. Tyle wystarczy, żeby odebrać przeciwnikowi większość tego, po co przychodzi.

Rozdział 31. Sektor prywatny i infrastruktura krytyczna: dlaczego to już wasza sprawa

Chcę zamknąć część systemową twierdzeniem, które nie wszystkim się podoba. Obrona przed rosyjską kampanią hybrydową w Europie nie jest już wyłącznie zadaniem państwa. W dużej części spadła na sektor prywatny i firmy ochrony, i to zanim ktokolwiek ich o to zapytał.

Powód jest prosty i wynika z celów przeciwnika. Cele leżą tam, gdzie jest logistyka wsparcia dla Ukrainy, energetyka, kolej, magazyny, węzły przeładunkowe, zakłady. Większość tej infrastruktury jest w rękach prywatnych albo chroniona przez prywatne firmy. Państwo nie postawi żołnierza przy każdym magazynie i przy każdym kilometrze toru, co pokazała zresztą sprawa Mika i Puławy, gdzie po ataku trzeba było mobilizować tysiące ludzi do dozoru odcinków, których normalnie nikt nie pilnuje. Na co dzień pierwszą i często jedyną warstwą obrony jest ochrona obiektu i jego personel. Czyli wy.

To jest zmiana roli, której branża jeszcze nie do końca przyjęła. Przez lata ochrona fizyczna była traktowana jako koszt, jako portier i kamera, jako coś, co ma odstraszyć złodzieja i spisać szkodę. Teraz ta sama ochrona jest pierwszą linią wobec obcego wywiadu prowadzącego rozpoznanie i sabotaż. To nie jest awans, o który ktokolwiek prosił, ale jest faktem, i lepiej go przyjąć świadomie niż zderzyć się z nim w noc, w którą coś się stanie.

Oceniam, że najtańszą i najskuteczniejszą inwestycją, jaką firma może zrobić, nie jest sprzęt, tylko świadomość personelu i zszycie warstw. Sprzęt jest drogi i szybko się starzeje. Przeszkolony człowiek, który rozpoznaje rozpoznanie i wie, jak zgłosić, jest tani i nie starzeje się wcale. Cała ta książka jest w gruncie rzeczy argumentem za tą jedną inwestycją.

Jest też strona, o której trzeba powiedzieć wprost, bo dotyczy pieniędzy i odpowiedzialności. Ramy prawne po 2022 roku zaostrzyły się na tyle, że sabotaż na rzecz obcego państwa jest ścigany jako ciężkie przestępstwo, a od operatorów infrastruktury krytycznej coraz częściej wymaga się realnych, nie papierowych, środków ochrony. Firma, która potraktuje to poważnie, zyskuje nie tylko bezpieczeństwo, ale i pozycję wobec regulatora i ubezpieczyciela. Firma, która potraktuje to jak kolejny audyt do odhaczenia, dowie się o różnicy w najgorszym możliwym momencie.

Czego nie wiem. Nie wiem, jak szybko regulacja dogoni rzeczywistość i czy zrobi to mądrze, czy przez kolejne formularze. Nie wiem, ile firm w Polsce ma dziś realną warstwę czujników, a ile ma ją tylko w prezentacji dla zarządu. Podejrzewam, że rozziew jest duży, ale tego nie zmierzyłem. Wiem tyle, że przeciwnik już wybrał cele, i że wiele z nich pracuje pod szyldami prywatnymi, nie państwowymi. Kto chroni taki obiekt, jest w tej grze, niezależnie od tego, czy się na nią pisał.

Rozdział 32. Dziesięć rzeczy do zapamiętania

Zamiast klasycznego zakończenia zostawiam listę, do której można wracać. Dziesięć zdań, które streszczają całość i które warto mieć w głowie, gdy zamknie się tę książkę.

Pierwsze. Po 2022 roku przewaga wróciła do obrońcy, bo przeciwnik zszedł na masowy, cyfrowy model, który zostawia ślady. Trzeba tę przewagę wziąć, sama się nie weźmie.

Drugie. Atak jest dziś synergiczny, składany z warstw cyfrowej, finansowej, fizycznej i ludzkiej. Obrona, która patrzy jedną warstwą, przegapi operację wchodzącą inną.

Trzecie. Klasyczna martwa skrzynka w dużej mierze ustąpiła miejsca Telegramowi, kryptowalucie i łańcuchowi kurierskiemu, ale logika została ta sama: rozdzielić, zaprzeczyć, przetrwać obserwację.

Czwarte. Główny wykonawca to dziś często amator zwerbowany przez czat, nieświadomy, dla kogo pracuje, groźny przez nieprzewidywalność, ale wykrywalny przez ślady.

Piąte. Werbunek ma sześć faz i najskuteczniej przerywa się go między pierwszą a drugą, zanim padnie pierwsze niewinne zadanie, które zamieni się w haczyk.

Szóste. Pojedynczy sygnał to nie dowód. Liczy się zbieg wielu wskaźników i odstępstwo od znanej normy. Kto nie zna normy, nie zobaczy anomalii.

Siódme. Rola obrońcy ma granicę: rozpoznaj, zabezpiecz, zgłoś. Nie ścigaj, nie konfrontuj, nie dotykaj, nie prowadź własnego śledztwa. Ta granica chroni dowody i ludzi.

Ósme. Zgłaszaj fakty, nie etykiety, i wąskim kanałem, nie do wszystkich. To chroni zgłaszającego, osobę niewinną i ewentualne działania służb naraz.

Dziewiąte. Najsłabszym i najsilniejszym punktem jest człowiek. Werbunek celuje w ludzi pod presją. Obrona buduje się przez wsparcie i zaufanie, nie przez inwigilację własnych.

Dziesiąte. Skuteczna obrona nie wymaga umiejętności ataku. Wymaga uwagi, procedury i dyscypliny. Te trzy rzeczy są w zasięgu każdej organizacji, która zdecyduje się je zbudować.

Stan na wrzesień 2026. Reszta zależy od tego, kto pierwszy zszyje swoje warstwy. Oby my.

Matthew Halaba halaba.online

DODATKI

Dodatek A. Kalendarium incydentów 2022–2026

Wybór najważniejszych, publicznie udokumentowanych zdarzeń istotnych dla tematu. Daty i ustalenia za źródłami z bibliografii; przy sprawach sądowych podano stan na wrzesień 2026.

2022

- 24 lutego, pełnoskalowa inwazja Rosji na Ukrainę; cezura dla całego opracowania.
- Marzec i dalej, skoordynowane wydalenia setek rosyjskich oficerów pod przykryciem dyplomatycznym z państw zachodnich; załamanie rezydentur legalnych SWR i GRU.
- 2022, Holandia demaskuje i zawraca Siergieja Czerkasowa (Victor Muller Ferreira), nielegała zmierzającego do MTK w Hadze.
- Grudzień, Słowenia aresztuje Annę i Artioma Dulcewów (María Mayer / Ludwig Gisch), nielegałów SWR.

2023

- Trwa demaskacja nielegałów w różnych krajach (m.in. wątek norweski, José Assis Giammaria).
- Christo Grozev/Bellingcat ustalają prawdziwe tożsamości Dulcewów i Olgi Kołobowej (Maria Adela / Neapol).

2024

- Marzec, podpalenie magazynu pomocy i sprzętu Starlink dla Ukrainy w Leyton (Londyn), zlecone przez Grupę Wagnera.
- Maj, pożar magazynu IKEA w Wilnie (powiązany z kampanią sabotażu).
- Lipiec, paczki zapalające w węzłach kurierskich (Lipsk, Birmingham, Polska); przechwycenia w Amsterdamie; przesyłki testowe do USA i Kanady.
- Sierpień, wielka wymiana więźniów w Ankarze; Dulcewowie wracają do Rosji, wita ich Putin.

2025

- Lipiec, brytyjski sąd skazuje sprawców podpalenia w Leyton (proces).
- Wrzesień, Wielka Brytania zatrzymuje trójkę podejrzanych o sabotaż na rzecz Rosji; NATO uruchamia Eastern Sentry po naruszeniach przestrzeni powietrznej przez drony; Niemcy startują z kampanią „Kein Wegwerf-Agent” (2 września).
- Październik, wyroki w sprawie Leyton (7–17 lat, pierwsze skazania z NSA 2023); Polska informuje o kolejnych zatrzymaniach w ramach kampanii przeciw dywersji.
- 16–17 listopada, sabotaż linii kolejowej Warszawa–Lublin–Hrubieszów (Mika, Puławy); najwyższy poziom alarmu politycznego w Polsce.
- 2 grudnia, zarzuty dla obywatela Rosji jako organizatora siatki sabotażowej powiązanej z FSB.

- Rok 2025, czeska BIS ujawnia sprawę Natalii Sudliankowej (GRU); seria uszkodzeń kabli bałtyckich; NATO, Baltic Sentry.

2026

- Kwiecień, start procesu w Wilnie (paczki zapalające, 5 oskarżonych); ujawnienie rozbicia międzynarodowej siatki zabójstw i sabotażu (Litwa, udział Ukrainy).
- Lipiec, Brazylia orzeka deportację Czerkasowa (30-letni zakaz wjazdu); Włochy zatrzymują dwie osoby ws. szpiegostwa na rzecz Rosji.
- Sierpień, wyrok w Stuttgarcie (paczki z GPS); dron z ładunkiem przy samolocie cargo w Lipsku-Halle.
- Do połowy 2026, analitycy odnotowują ~czterokrotny wzrost operacji sabotażowych względem 2024; prognozy dalszej eskalacji.

Dodatek B. Struktura rosyjskich służb specjalnych (w zakresie istotnym dla tematu)

Uproszczony przewodnik. KGB specjalizowało się w mylącej terminologii i częstych zmianach nazw; poniżej wersja funkcjonalna, wystarczająca dla czytelnika defensywnego.

SWR (Służba Wywiadu Zagranicznego). Cywilny wywiad zagraniczny, spadkobierca Pierwszego Zarządu Głównego KGB. Historycznie prowadzi program nielegałów przez komórkę o tradycji Zarządu „S". Z SWR kojarzone są klasyczne siatki nielegałów (Ghost Stories 2010) oraz część współczesnych nielegałów (Dulcewowie).

GRU / GU (wywiad wojskowy). Odrębny od SWR pion wojskowy. Historycznie prowadził własny program nielegałów. Z GRU wiąże się **jednostka 29155**, kojarzona z sabotażem, zamachami i zabójstwami za granicą (Vrbětice 2014, Salisbury 2018), a po 2022 roku, z organizowaniem sabotażu rękami pośredników. Sprawy Kołobowej i Giammarii przypisywano GRU.

FSB (Federalna Służba Bezpieczeństwa). Głównie kontrwywiad i bezpieczeństwo wewnętrzne, ale po 2022 roku coraz aktywniejsza w operacjach zagranicznych, zwłaszcza na kierunku ukraińskim i w werbunku wykonawców sabotażu (sprawa Mika/Puławy przypisana FSB).

Uwaga o rozmyciu granic. Po 2022 roku podział kompetencji się rozmywa: FSB działa za granicą, GRU sięga po lokalnych pośredników, a nieformalne struktury (jak dawna Grupa Wagnera czy „fabryki trolli" typu IRA) realizują zadania, które w ZSRR należałyby do jednej służby. Dla obrońcy dokładne przypisanie sprawy konkretnej służbie jest wtórne, liczy się rozpoznanie wzorca działania, nie etykieta organizacyjna.

Dodatek C. Zbiorcza karta wskaźników rozpoznania (do wydruku)

GRUPA A, WERBUNEK - Niezamówiona oferta pieniędzy za „drobne zadania” (komunikator / media społ.). - Zadania: fotografuj obiekt / przewieź / nadaj paczkę / oznacz miejsce, bez uzasadnienia. - Nacisk na szyfrowany komunikator i dyskrecję od początku; wymóg filmowania. - Pośrednik zamiast pracodawcy; płatność w krypto. - U pracownika: nagłe zainteresowanie grafikami/dostępem/przesyłkami; nagła zmiana finansów; podatność na szantaż.

GRUPA B, ROZPOZNANIE OBIEKTU - Fotografowanie/filmowanie zabezpieczeń (kamery, brama, posterunek, ogrodzenie), zwłaszcza powtarzalne. - Pytania o procedury, grafiki, obsadę, dostawy, godziny. - Powtarzalna obecność osób/pojazdów bez powodu; testowanie reakcji ochrony. - Drony nad/przy obiekcie.

GRUPA C, ŁĄCZNOŚĆ BEZOSOBOWA / PODŁOŻENIE - Przedmiot „nie na miejscu”; zbyt czysty/nowy jak na otoczenie. - Powtarzalny, bezsensowny znak/przedmiot w rytmie skorelowanym z czyimś zachowaniem. - Krótka czynność przy elemencie otoczenia i odejście. - Nietypowa przesyłka: anonimowy nadawca, „testowa”, anomalia wagi/zapachu/wycieku/temperatury/dźwięku.

GRUPA D, GŁĘBOKIE PRZYKRYCIE (NIELEGAŁ) - Konsekwentne unikanie fotografii. - „Firma” pretekstowa, uboga, głównie jako uzasadnienie podróży/obecności. - Duża gotówka bez pokrycia. - Gładka, nieweryfikowalna biografia z odległego kraju; akcent niepasujący do pochodzenia. - Kontakty ukierunkowane na osoby z dostępem, nieproporcjonalnie do zawodu.

ZASADY (na odwrocie karty) 1. Anomalia na tle znanej normy. 2. Wiele wskaźników, nie jeden. 3. Granica roli: obserwuj–zabezpiecz–zgłoś. 4. Zgłoszenie bez etykietowania. 5. Bez profilowania po narodowości/wyglądzie.

REAKCJA NA PRZEDMIOT: 4×NIE (nie dotykaj / nie otwieraj / nie przemieszczaj / nie używaj radia tuż przy) + 3×TAK (strefa i ludzie / powiadom służby / udokumentuj + CCTV).

ZGŁOSZENIE (PL): ABW oraz policja; bezpośrednie zagrożenie, 112. Kanał wąski i imienny.

Dodatek D. Bibliografia i źródła

Książka źródłowa

- Shaun Walker, *Nielegałowie. Jak szpieguje nas Rosja*, wyd. polskie (na podstawie *The Illegals*, 2025). Rozdziały wykorzystane w szczególności: Wprowadzenie; rozdz. 25 „Operacja Ghost Stories"; rozdz. 26 „Wirtualni nielegałowie"; Posłowie; Dodatki (terminologia i struktura KGB).

Raporty i komunikaty służb oraz instytucji

- Agencja Bezpieczeństwa Wewnętrznego (ABW), jawny raport roczny 2024–2025 (dane o śledztwach i zarzutach; profesjonalizacja i płatności w krypto).
- BKA / BND / BfV / BAMAD, wspólna kampania informacyjna „Kein Wegwerf-Agent werden!" (2 września 2025).
- SUPO (Finlandia), „How to recruit a saboteur" (sześciofazowy model werbunku).
- BIS (Czechy), ustalenia o werbunku migrantów przez Telegram i strategicznych celach operacji; sprawa N. Sudliankowej (2025).
- Crown Prosecution Service (Wielka Brytania), komunikaty ws. sprawy Leyton i zastosowania National Security Act 2023.
- Counter Terrorism Policing (Wielka Brytania), komunikaty o wyrokach (październik 2025).
- Rada UE / EEAS (Consilium), komunikaty o reżimie sankcji za rosyjskie zagrożenia hybrydowe (2025–2026).
- U.S. Senate Select Committee on Intelligence, Annual Threat Assessment 2026 (wzmianka o sabotażu kolejowym w Polsce).
- NATO / SHAPE, Baltic Sentry, Eastern Sentry.
- NPSA (Wielka Brytania), materiały o ryzyku wewnętrznym (insider risk).

Dziennikarstwo śledcze i OSINT

- Christo Grozev / Bellingcat, demaskacje nielegałów (Dulcewowie, O. Kołobowa) oraz oficerów GRU (Salisbury).
- OCCRP, „Make a Molotov Cocktail: How Europeans Are Recruited Through Telegram…".
- The Insider, o werbunku przez Telegram i stawkach.
- Propastop, „Russia's Shadow Army in Europe…" (model werbunku).

Analizy i think tanki

- Carnegie Europe, o eskalacji działań hybrydowych w 2026.
- GLOBSEC, aktualizacja raportu o „crime-terror nexus" i prognozy na 2026.
- FOI (Szwecja), analiza 70 wyroków za szpiegostwo w Europie (2008–2024): typologie agentów, motywacje (MICE), werbunek cyfrowy.
- Congressional Research Service, o rosyjskich działaniach hybrydowych w Europie.
- Atlantic Council, CEPA, JSIS (UW), o bezpieczeństwie kabli bałtyckich i odpowiedzi państw.

Materiały prasowe (wybór)

- Reuters, CNN, Euronews, Al Jazeera, RFE/RL, Kyiv Independent, Notes from Poland, PAP, Infosecurity24, relacje ze spraw: Leyton, paczki DHL, Mika/Puławy, proces wileński, sprawa Czerkasowa, zatrzymania we Włoszech, drony (Lipsk).

> **Nota o źródłach.** Opracowanie opiera się wyłącznie na materiałach jawnych. Przy sprawach będących w toku obowiązuje domniemanie niewinności; podane ustalenia odzwierciedlają stan publicznej wiedzy na wrzesień 2026 i mogą ulec zmianie w toku postępowań. Tam, gdzie źródła były niepewne lub sprzeczne, zaznaczono to w tekście.

Przypisy

Opracowanie ma charakter przeglądowo-szkoleniowy i posługuje się przypisami zbiorczymi do części i rozdziałów, odsyłającymi do pozycji z Dodatku D.

1. Część I (rozdz. 1–5), na podstawie: Walker, *Nielegałowie*, Wprowadzenie oraz rozdz. o życiu nielegałów i sprawie Ghost Stories; klasyczne sprawy (Fisher/Abel, Portland, Hanssen) za literaturą przedmiotu wskazaną przez Walkera.
2. Rozdz. 6, Walker, Posłowie (wydalenia dyplomatów, załamanie rezydentur, zwrot ku nielegałom); Carnegie Europe (2026), wzrost liczby operacji sabotażowych.
3. Rozdz. 7, Walker, Posłowie (Czerkasow, Dulcewowie, Kołobowa, wymiana w Ankarze 2024, cytaty źródła moskiewskiego); Bellingcat/Grozev (identyfikacje); RFE/RL i in. (deportacja Czerkasowa 2026).
4. Rozdz. 8, Walker, rozdz. 26 (jednostka 29155, Vrbětice, Salisbury); GLOBSEC (crime-terror nexus); BIS (cele strategiczne).
5. Rozdz. 9, SUPO (model sześciofazowy); OCCRP, The Insider, Propastop (werbunek przez Telegram); BKA/BfV/BND/BAMAD (kampania „Kein Wegwerf-Agent", 2 września 2025).
6. Rozdz. 10, Euronews/Reuters (paczki z GPS, wyrok Stuttgart 2026); relacje o paczkach zapalających 2024; BIS (płatności w krypto); Walker, Posłowie (gotówka w sprawie Dulcewów).
7. Rozdz. 11, ABW, raport 2024–2025 (liczby); PAP, Infosecurity24 (komentarze); przeglądy incydentów w DE/UK/CZ/EE/LV/NO/IT; NATO (Baltic/Eastern Sentry).
8. Rozdz. 12, CPS i Counter Terrorism Policing (Leyton, wyroki 2025); Euronews/CNN (paczki DHL, proces wileński 2026); Wikipedia/Notes from Poland/RFE-RL/PBS (Mika/Puławy 2025); Pravda/Reuters (siatka zabójstw 2026); Stuttgart (GPS 2026); Walker (Dulcewowie).
9. Rozdz. 13, synteza źródeł z rozdz. 9–12; FOI (typologie i werbunek cyfrowy).
10. Część III (rozdz. 14–20, moduły A–B), synteza modeli SUPO, NPSA (insider risk) i praktyki opisanej w źródłach; scenariusze na kanwie spraw z rozdz. 12.
11. Część IV (rozdz. 21–25), jak wyżej, z uzupełnieniem: CPS/NSA 2023 (UK); Consilium/EEAS (sankcje UE); ATA 2026 (USA); Carnegie, GLOBSEC (prognozy); Atlantic Council, CEPA (infrastruktura).

Koniec opracowania. Stan na wrzesień 2026.